9. THE PLA AND INFORMATION WARFARE

James Mulvenon

INTRODUCTION

Among recent discussions of the evolution of Chinese military doctrine, few subjects have received as much attention as information warfare (IW).[1] China is arguably only one of three countries pushing the envelope on IW strategy development, behind the United States and Russia.[2] It has an active offensive IW program and has devoted significant resources to the study of IW. Chinese military journals are replete with articles that either directly or indirectly address the subject, and a significant number of full books by PLA authors have been published in the past few years.[3] Granted, IW's current cachet in both China and the United States can be partly explained by the hip, futuristic, attractively ill-defined nature of the subject, which invites the frenetic pace at which some of the nation's most forward thinkers are attempting to coin the permanent neologisms and concepts of this new type of combat.[4] At the same time, however, I would argue that behind all the rhetoric and hype, IW presents

---

[1]Two good introductions to the subject are Bates Gill, *China and the Revolution in Military Affairs*, Carlisle, PA: Strategic Studies Institute, 1996; and John Arquilla and Solomon Karmel, "Welcome to the Revolution . . . in Chinese Military Affairs," *Defense Analysis*, 13:3, December 1997, pp. 255–269.

[2]For an excellent cross-section of U.S. writings on the subject, see John Arquilla and David Ronfeldt (eds.), *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica, Calif.: RAND, MR-880-OSD/RC, 1998. See also Martin Libicki, *What Is Information Warfare?* Washington, DC: National Defense University Press, 1996; John Arquilla and David Ronfeldt, "Cyberwar Is Coming!" *Comparative Strategy* 12, No. 2, Spring 1993, pp. 141–165; Richard Szafranski, "A Theory of Information Warfare," *Airpower Journal*, Spring 1995, pp. 56–65; Alan Campen *et al.*, *Cyberwar*, Washington, DC: AFCEA Press, 1996; Norman Davis, "An Information-Based RMA," *Strategic Review*, Winter 1996; C. Kenneth Allard, "The Future of Command and Control Warfare: Toward a Paradigm of Information Warfare," in L. Benjamin Ederington and Michael Mazarr (eds.), *Turning Point: The Gulf War and U.S. Military Strategy*, Boulder, Colo.: Westview Press, 1995. For the best summary of Russian IW writings, see the work of Timothy Thomas.

[3]Among books, the most notable are Wang Pufeng, *Xinxi zhanzheng yu junshi geming* (Information Warfare and the Revolution in Military Affairs), Beijing: Junshi kexueyuan, 1995; Shen Weiguang, *Xin zhanzheng lun* (On New War), Beijing: Renmin chubanshe, 1997; Wang Qingsong, *Xiandai junyong gaojishu* (Modern Military-Use High Technology), Beijing: AMS Press, 1993; Li Qingshan, *Xin junshi geming yu gaojishu zhanzheng* (New Military Revolution and High Tech War), 1995; Zhu Youwen, Feng Yi, and Xu Dechi, *Gaojishu tiaojianxia de xinxizhan* (Information War Under High Tech Conditions), Beijing: AMS Press, 1994; Zhu Xiaoli and Zhao Xiaozhuo, *Mei'E xin junshi geming* (The United States and Russia in the New Military Revolution), Beijing: AMS Press, 1996; Dai Shenglong and Shen Fuzhen, *Xinxizhan yu xinxi anquan zhanlue* (Information Warfare and Information Security Strategy), Beijing: Jincheng Publishing House, 1996.

[4]One can identify a similar dynamic in the early years of the literature on nuclear strategy. See Fred Kaplan, *The Wizards of Armageddon*, New York: Simon and Schuster, 1983.

the Chinese with a potentially potent, if circumscribed, asymmetric weapon. Defined carefully, it could give the PLA a longer-range power projection capability against U.S. forces that its conventional forces cannot currently hope to match. In particular, I would argue that these weapons give the PLA a possible way to attack the Achilles' Heel of the advanced, informatized U.S. military: its information systems, especially those related to command and control and transportation. By attacking these targets, the Chinese could possibly degrade or delay U.S. force mobilization in a time-dependent scenario, such as Taiwan, and do so with a measure of plausible deniability.

This paper seeks to outline the current debate within the PLA over information warfare, emphasizing its remarkably heterogeneous character. It draws upon a sizable number of full-length books and journal articles. What this paper does *not* do, however, is assess PLA capabilities in information warfare, since nearly all of the relevant data resides in the classified realm. Nonetheless, this literature analysis is an important first step in understanding the role of information warfare in the 21st century PLA.

DEFINING TERMS

Before proceeding further, it is necessary to define terms, although this exercise is fraught with terminological, political, and ideological peril. In some ways, however, the Chinese themselves have made the job a little easier. Chinese writings clearly suggest that IW is a solely military subject, and as such, they draw inspiration primarily from U.S. military writings. The net result of this "borrowing" is that many PLA authors' definitions of IW and IW concepts sound eerily familiar. For our purposes, therefore, we shall use the definition of information warfare found in Joint Pub 3-13, *Joint Doctrine for Information Operations (IO)*:

> Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.[5]

"Information operations" are defined in Joint Pub 3-13.1, *Joint Doctrine for Command and Control Warfare (C2W)* as:

> actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks, while defending one's own information, information-based processes, information systems, and computer-based networks.[6]

More concretely, the Army in FM-100-6 *Information Operations* defines "information operations" as

> continuous military operations within the military environment that enable, enhance, and protect the friendly force's ability to collect, process, and act on

---

[5]Joint Chiefs of Staff (JCS) Pub 3-13, *Joint Doctrine for Information Operations (IO)*, October 9, 1998, p. I9.

[6]Joint Chiefs of Staff (JCS) Pub 3-13.1, *Joint Command and Control Warfare (C2W) Operations*, February 7, 1996, p. I3.

> information to achieve an advantage across the full range of military operations; information operations include interacting with the global information environment and exploiting or denying an adversary's information and decision capabilities.[7]

The goal of these operations is "information dominance," or

> The degree of information superiority that allows the possessor to use information systems and capabilities to achieve an operational advantage in a conflict or to control the situation in operations short of war, while denying those capabilities to the adversary.[8]

By introducing these definitions, I am not precluding that the Chinese may eventually develop an indigenous IW strategy, and there is limited evidence of movement in this direction. Instead, these U.S. definitions provide a baseline by which to judge PLA writings.

CHINESE INFORMATION WARFARE STRATEGY: HETEROGENEITY AND INNOVATION

This section examines the early-stage Chinese IW literature, offering the following preliminary conclusions.

The literature:

- focuses on disrupting logistics and communications
- understands the U.S. threat and admits their own technical weaknesses, including poor reliability, survivability, and security
- reveals a surprising grasp of U.S. IW doctrine, but borrows concepts inappropriate for the PLA's technological level
- correctly identifies the important lessons of DESERT STORM, but in some cases draws the wrong conclusions
- overestimates Chinese capabilities to develop effective defensive countermeasures.

Evolution of Chinese IW Strategy

In the mythology of PLA IW study, Shen Weiguang, a soldier in a field unit, began writing about information warfare in 1985, publishing a book entitled *Information Warfare* that was later excerpted as an article in *Liberation Army Daily*.[9] Chinese IW doctrine did not achieve an analytical focus, however, until the Gulf War in 1991. As has been documented in many other places, the Chinese military leadership was very

---

[7]Field Manual 100-6 *Information Operations*, August 1996.

[8]Ibid., p. 8.

[9]Shen Weiguang, "Focus of Contemporary World Military Revolution—Introduction to Information Warfare," *Jiefangjun bao*, November 7, 1995, p. 6.

impressed by the performance of U.S. forces in DESERT STORM, especially the ease with which they destroyed the Iraqi's largely Soviet and Chinese equipment. From their writings, it seems clear that PLA theorists believe that IW played a significant role in the U.S. victory. A commonly held belief, for example, is that the U.S. military used computer viruses to disrupt and destroy Iraqi information systems.[10] In their descriptions of DESERT STORM, these authors point to other allied operations and technologies as examples of information war. First, Wang Pufeng singles out superior satellite reconnaissance of strategic sites and Iraqi positions, as well as attacks on Iraqi command and control systems, as key elements of the rapid allied victory against Saddam's forces.[11]

On the lessons of DESERT STORM for the PLA, however, there is some divergence between those who believe the next war will look just like the Gulf War and those who understand that the Gulf War was a testing ground for advanced weapons and strategy to be used in a future, different war. Most seem awed by the "perfect" [*wanshan*] execution of the attack.[12] One writer described the new changes in information, command and control brought about by the Gulf War as a "great transformation" [*zhongda biange*],[13] and a second suggested that strategies to defend and attack computers and electronic systems could be as significant in determining the outcome of future wars as strategies to defend and attack citizens were in past wars.[14] Finally, Wang Pufeng called the Gulf War the "epitome" of information war.[15]

Since DESERT STORM, Chinese IW research has rapidly proliferated in newspapers, journals, and books. Some of the most prominent IW researchers and their billets are listed in Table 1 below.

Table 1

Important Chinese IW Theorists

Theorist	Billet/Comments
MG Wang Pufeng	Father of Chinese IW field Seminal work: *Information Warfare and the Revolution in Military Affairs*
Shen Weiguang	State Council Special Economic Zones Office (former PLA)
Wang Baocun	Academy of Military Sciences
Li Fei	*Liberation Army Daily*
Wang Xusheng	PLA Academy of Electronic Technology
Su Jinhai	PLA Academy of Electronic Technology
Zhang Hong	PLA Academy of Electronic Technology

[10]"Army Paper on Information Warfare," *Jiefangjun bao*, 25 June 1996, p. 6.

[11]Wang Pufeng, pp. 113–116; 123–126.

[12]Ibid., p. 203.

[13]Liu Yichang (ed.), *Gaojishu zhanzheng lun* (On High-Tech War), Beijing: Military Sciences Publishing House, 1993, p. 272.

[14]Li Zhisun and Sun Dafeng, *Gaojishu zhanzheng molü* (The Strategy of High-Tech War), Beijing: Defense University Publishing House, 1993, pp. 3–9, 184–201.

[15] Wang Pufeng, p. 144.

In addition, it has become increasingly obvious that some IW "centers of excellence" are emerging in the PLA. These centers are listed in Table 2 below.

These researchers began to congregate at a series of high-level scholarly meetings. In December 1994, the Commission of Science, Technology, and Industry for National Defense (COSTIND) sponsored a symposium entitled "Analysis of the National Defense System and the Military Technological Revolution," which was closely followed by an October 1995 meeting that dealt with "The Issue of Military Revolution." The alleged high point of Chinese IW research was a 22 December 1995 COSTIND National Directors conference, when Liu Huaqing allegedly stated:

> Information warfare and electronic warfare are of key importance, while fighting on the ground can only serve to exploit the victory. Hence, China is more convinced [than ever] that as far as the PLA is concerned, a military revolution *with information warfare as the core* has reached the stage where efforts must be made to *catch up with and overtake rivals*. (emphasis added)[16]

More recently, a group of 40 information warfare researchers met in Shenyang for a *Junshi xueshu* symposium on information warfare. The researchers, who were drawn from relevant departments of the army's general departments, military regions, armed services, scientific research institutions, academies, and units, discussed the "nature, position, role, guiding ideology, principles, modes, methods, and means" of information warfare.[17]

Table 2

Major Centers of IW Research

Center	Comments
Academy of Military Sciences Military Strategy Research Center	Main IW research center Developing IW strategies Integrating IW into overall military doctrine Dedicated to "winning information warfare in the information age" Affiliated with the Society for International Information Technologies
PLA Academy of Electronic Technology	
General Staff Department Third Sub-Department (GSD/3rd)	IW work carried out by Research Institute 61 and Information Engineering Academy
China National Research Center for Intelligence Computing Systems	
COSTIND University of Electronic Science and Technology (Chengdu)	

16"Latest Trends in China's Military Revolution," *Hsin Pao* [*Hong Kong Economic Journal*].

17Li Pengqing and Zhang Zhanjun, "Explore Information Warfare Theories with PLA Characteristics—*Junshi xueshu* Magazine Holds Symposium," *Jiefangjun bao*, 24 November 1998, p. 6, in FBIS-CHI-98-349, December 15, 1998.

Important Chinese IW Concepts and Terms: Definitions

When examining Chinese IW theories, the logical place to start is Wang Pufeng's seminal work, *Information Warfare and the RMA*. Wang defines information warfare as follows:

> 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.[18]

Later, the author elaborates his definition:

> Information war is a crucial stage of high-tech war. . . . At its heart are information technologies, fusing intelligence war, strategic war, electronic war, guided missile war, a war of "motorization" [*jidong zhan*], a war of firepower [*huoli*]—a total war. It is a new type of warfare.

The author distinguishes this new type of warfare from the previous paradigm:

> Information and the capacity [to employ it] together release new energy in battle; information's "networkization" opens up a new battlefield of computers. With the "informationization" [*xinxihua*] of the army, agility and speed, mobility, and depth of attack, in a battle without a front line, all create a leap ahead of the traditional methods of warfare. The area [of the battle] grows, its speed increases, the accuracy of the attack is more acute, all of which change past conceptions of space and time.[19]

It is important to note that nothing in these definitions conflicts with American military conceptions of information warfare.

Important Chinese IW Concepts and Terms: Principles

The aim of IW in the Chinese literature is information dominance [*zhixinxiquan*], defined as the ability to defend one's own information while exploiting and assaulting an opponent's information infrastructure.[20] This information superiority has both technological and strategic components. On the one hand, it requires the ability to interfere with an enemy's ability to obtain, process, transmit, and use information to paralyze his entire operational system. This accords with U.S. military conceptions of information dominance. On the other hand, some Chinese commentators assert that information superiority is not determined by technological superiority, but by new tactics and the independent creativity of commanders in the field, placing much more emphasis on personnel and organization-related components of the conflict.

---

[18]Wang Pufeng, p. 37.

[19]Ibid., p. 2.

[20]This section draws from MAJ Mark Stokes' excellent study, *China's Strategic Modernization*.

The information battlefield itself is transformed in the PLA literature. Concepts of front and rear battlelines blur as the "multidimensional" battlefield space, integrating air, land, sea, space, and the electronic spectrum, becomes the arena of combat.[21] Within this battlefield, military units conduct "seamless operations" [*feixianxing zuozhan*], integrating sensors with weapons systems. Operational emphasis is placed on deep strike [*zongshen zuozhan*] and over-the-horizon warfare [*yuanzhan*] against command and control facilities, which are perceived to be the "vital points" [*dianxue*] of the system. The objectives of the operation are not the seizing of territory or the killing of enemy personnel, but rather the destruction of the other side's willingness to resist.

Victory on this information battlefield will shift the focus of operations. In the words of two PLA authors,

> the key to gaining the upper hand on the battlefield is no longer mainly dependent on who has the stronger firepower, but instead depends on which side discovers the enemy first, responds faster than the latter, and strikes more precisely than the latter. [The two sides] vie for the advantage in intelligence and command control, i.e. to see which side holds a larger amount of and more accurate information and is faster in transmitting and processing the information. On the other hand, they have to vie for advantage in the precision of the strike, i.e., to see which side can hit the other at a longer distance and hit the other side first at the same distance.[22]

As a consequence, detection, concealment, search and avoidance become central goals, pushing the military towards networked command and smaller, modular units.

Something Borrowed, Something Blue

One of the problems in analyzing PLA IW strategy, however, is disaggregating it from translations or outright copying of U.S. doctrinal writings, as well as Russian, German and French sources.[23] From conversations in Beijing, it is clear that the PLA has translated both FM-100-6, *Information Operations*, and JP 3-13.1, *Joint Doctrine for Command and Control Warfare*, along with a myriad of lesser documents, journal articles, and policy papers, including more abstract research on information revolution written by the Tofflers, David Ronfeldt, John Arquilla, and Martin Libicki. PLA writings selectively steal concepts and definitions from these works, though it is rare that doctrine is adopted wholesale. As a result, the terminology, definitions, and even case studies found in most Chinese writings are similar to the debate in the United States. A sample is presented in the next three paragraphs, though one could easily add hundreds of additional examples to this list.[24]

---

[21] Wang Jianghuai and Lin Dong, "Viewing Our Army's Quality Building from the Perspective of What Information Warfare Demands," *Jiefangjun bao*, March 3, 1998, p. 6, in FBIS-CHI-98-072, March 13, 1998.

[22] Ibid.

[23] Wang Pufeng, p. 141.

[24] For an article which is almost entirely derivative, see Wang Baocun and Li Fei, "An Informal Discussion of Information Warfare (Parts One, Two and Three)," *Jiefangjun bao*, June 13, 1995.

For example, at the highest level of abstraction, one PLA author describes the information age as the third important age in world history, following the agricultural age and the Industrial revolution.[25] Furthermore, he characterizes the defining feature of the latter part of the information age as the exponential increase in "data production, storage, exchange, and transmission." Both of these ideas are taken without attribution directly from the Tofflers' seminal futurist books *The Third Wave*[26] and *War and Anti-War*,[27] respectively.

In an example of direct appropriation of U.S. military operational doctrine, one PLA author defined the aim of IW as "preserving oneself and controlling the enemy," the core distillation of the U.S. military's concept of "information dominance."[28] Moreover, the same author asserted that IW included "electronic warfare, tactical deception, strategic deterrence, propaganda warfare, psychological warfare, computer warfare, and command and control warfare,"[29] which is virtually identical to the U.S. Air Force's doctrinal "Six Pillars of IW."

In conceptions of the information battlefield, the similarities continue. PLA authors discuss "integration" [*yitihua*] and seamless operations [*feixianxing zuozhan*], tying together the five dimensions of warfare—air, land, sea, space, and the electromagnetic spectrum—through the integration of sensors with mobile missiles, air, and sea-based forces. These sensors are meant to facilitate "dominant battlefield awareness," which in turn permits deep strike [*zongshen zuozhan*] against enemy command and control hubs, communication networks, and supply systems, blurring previous distinctions of a clear battleline.[30] For students of U.S. military doctrine, this conception of the battlefield is virtually identical to the core principles of Joint Vision 2010.[31]

The question, therefore, could be posed in the following manner: Is there a *Chinese* IW strategy? There are certainly important differences between the Chinese and American IW literatures. To summarize, PLA writers universally regard IW as a strictly military subject first and foremost, while Western authors largely accept the dichotomy between information warfare waged between states or militaries (i.e., cyberwar) and information warfare waged between substate actors and states (i.e., netwar).[32] Second, Chinese IW authors imbed their discussions within familiar ideological frameworks, such as Maoist guerrilla strategy and Sun Zi. In the Maoist

---

[25]Cai Renzhao, "Exploring Ways to Defeat the Enemy Through Information," *Jiefangjun bao*, March 19, 1996, p. 6.

[26]Alvin and Heidi Toffler, *The Third Wave*, New York: Bantam, 1980.

[27]Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century*, Boston: Little, Brown and Company, 1993.

[28]Su Enze, "Logical Concepts of Information Warfare," *Jiefangjun bao*, June 11, 1996, p. 6.

[29]Ibid.

[30]Cai Renzhao, "Exploring Ways to Defeat the Enemy Through Information," *Jiefangjun bao*, March 19, 1996.

[31]Office of the Joint Chiefs of Staff, *Joint Vision: 2010*, available at http://www.dtic.mil/doctrine/jv2010/jv2010.pdf.

[32]This distinction between cyberwar and netwar was coined by John Arquilla and David Ronfeldt. See *The Advent of Netwar*, Santa Monica, Calif.: RAND, MR-789-OSD, 1996.

vein, IW is referred to as the "New People's War," with particular attention paid to the idea of "overcoming the superior with the inferior." Both U.S. and Chinese authors are guilty of overusing Sun Zi, especially the notion of "winning the battle without fighting." While most of these references are nothing more than rhetorical flourishes, they do reflect two stark realities: (1) the extent to which Chinese (and U.S.) authors are struggling to find a framework for understanding IW and (2) the continuing pull of more traditional strategic frameworks. Third, Wang Pufeng and others emphasize the nontechnological aspects of information warfare to a much greater extent than U.S. military analysts, especially the need for new strategies and new organizational forms.[33] Fourth, Chinese IW theorists, by virtue of the PLA's relatively backward state, are forced by circumstance to discuss IW from the perspective of a technologically inferior military, often in opposition to a technologically advanced foe.

This latter point deserves further elaboration. One of the most interesting Chinese IW concepts is the notion of "overcoming the superior with the inferior," which draws inspiration from both Sun Zi and Maoist "People's War." A basic assumption of this line of reasoning is that the PLA will most likely face an opponent capable of achieving information dominance on the battlefield. In response, the PLA has two choices. The first is to adopt nontechnological measures to overcome technological disadvantage, such as camouflage, concealment, and deception techniques. While there is some merit in this argument, the experience of the Iraqi army in DESERT STORM does not foster much optimism that this strategy would be successful against a determined opponent.

The second choice is more interesting, and I would argue, should be much more worrisome to U.S. military planners. PLA writings generally hold that IW is an unconventional warfare weapon, not a battlefield force multiplier. Indeed, many writings suggest that IW will permit China to fight and win an information campaign, *precluding the need for military action*. When this train of thought is combined with the notions of "overcoming the superior with the inferior," one can quickly see the logical conclusion of the argument: IW as a preemption weapon.[34] According to Lu Linzhi,

> In military affairs, launching a preemptive strike has always been an effective way in which the party at a disadvantage may overpower its stronger opponent. . . . For the weaker party, waiting for the enemy to deliver the first blow will have disastrous consequences and may even put it in a passive situation from which it will never be able to get out . . .

As a concrete example, he points to the Gulf War, where Iraq's failure to launch a preemptive attack resulted in their defeat:

---

[33]This is not to say that Western authors do not emphasize the nontechnological aspects of information warfare. In fact, John Arquilla and David Ronfeldt are two prominent examples of American IW theorists who see the profound organizational and societal implications of IW and the information revolution writ large. See John Arquilla and David Ronfeldt (eds)., *In Athena's Camp*.

[34]Lu Linzhi, "Preemptive Strikes Crucial in Limited High-Tech Wars," *Jiefangjun bao*, February 14, 1996, p. 6.

> In the Gulf War, Iraq suffered from passive strategic guidance and overlooked the importance of seizing the initiative and launching a preemptive attack. In doing so, it missed a good opportunity to turn the war around and change its outcome.[35]

This accords with some Western military analysts, who argue that Iraq should have attacked Allied forces in Saudi Arabia at the early stage of the deployment rather than permitting the forces of the U.S. and the other members of coalition to deploy without hindrance over a six-month period.[36]

To avert this outcome, Lu states that an effective strategy by which the weaker party can overcome its more powerful enemy is

> to take advantage of serious gaps in the deployment of forces by the enemy with a high tech edge by launching a preemptive strike during the early phase of the war or in the preparations leading to the offensive.[37]

The reason for striking is that the "enemy is most vulnerable during the early phase of the war."[38] In terms of specific targets, the author asserts that

> we should zero in on the hubs and other crucial links in the system that moves enemy troops as well as the war-making machine, such as harbors, airports, means of transportation, battlefield installations, and the communications, command and control and information systems.[39]

If these targets are not attacked or the attack fails, the "high-tech equipped enemy" will amass troops and deploy hardware swiftly to the war zone, where it will carry out "large-scale airstrikes in an attempt to weaken . . . China's combat capability."[40]

HOW COULD THE CHINESE CREDIBLY USE IW? AN UNSETTLING SCENARIO INVOLVING THE UNITED STATES AND TAIWAN

In his discussion of IW as a preemption weapon, Lu Linzhi lays out a scenario in which China employs a preemptive strike to defeat a technologically superior enemy during the latter's mobilization and deployment phase. When one reads between the lines, it becomes readily apparent that the author is describing the rough parameters of a potential confrontation between China and the United States. This becomes even more clear in the following revealing passage, where he frankly discusses the technological imbalances between China and its thinly disguised "high-tech enemy":

> Reconnaissance positioning satellites, AWACs, stealth bombers, aircraft carriers, long-range precision guided weapons . . . the enemy has all that; we don't. As for tactical guided missiles, electronic resistance equipment, communications,

---

[35]Ibid.

[36]A discussion of the coalition forces' early vulnerabilities can be found in Michael Gordon and General Bernard Trainor, *The General's War*, Boston: Little, Brown, and Company, 1995, pp. 57–64.

[37]Lu Linzhi, "Preemptive Strikes."

[38]Ibid.

[39]Ibid.

[40]Ibid.

> command and control information systems, main battlefield aircraft, main battlefield tanks, and submarines, what we have is inferior to the enemy's.[41]

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.[42] American forces *are* highly information-dependent, and rely heavily on precisely coordinated logistics networks, such as those operated by TRANSCOM. 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. The advantages to this strategy are numerous: (1) it is available to the PLA in the near term; (2) it does not require the PLA to be able to attack/invade Taiwan with air/sea assets, which most analysts doubt the PLA is capable of achieving for the next ten years or more; and (3) it has a reasonable level of plausible deniability, provided that the attack is sophisticated enough to prevent tracing.[43]

CONCLUSION

To sum up, the available evidence suggests that the PLA does not currently have a coherent IW doctrine, certainly nothing compared to U.S. doctrinal writings on the subject. While PLA IW capabilities are growing, they do not match even the primitive sophistication of their underlying strategies, which call for stealth weapons, joint operations, battlefield transparency, long-range precision strike, and real-time intelligence. Yes, the PLA is acquiring advanced telecommunications equipment through its commercial operations, even BC4I gear, but it is not clear that this equipment or subcomponents are being incorporated into PLA units, much less integrated into the military's system as a whole. Therefore, IW may currently offer the PLA some attractive asymmetric options, some of which may be decisive in narrowly circumscribed situations, but the Chinese military cannot reasonably expect anything approaching "information dominance" for the foreseeable future.

---

[41] Ibid.

[42] Two PLA authors explicitly endorse what they call "asymmetric information offensives." See Wang Jianghuai and Lin Dong, "Viewing Our Army's Quality Building from the Perspective of What Information Warfare Demands," *Jiefangjun bao*, March 3, 1998, p. 6, in FBIS-CHI-98-072, March 13, 1998.

[43] The plausible deniability of a PLA IW attack will increase markedly by the end of 1998, when a Trans-Eurasian landline cable will be completed. Currently, all international Internet gateways out of China connect to the North American backbone. When the Trans-Eurasian connection is open, however, Chinese hackers will be able to "wipe" their IP headers in Europe, making it extremely difficult for U.S. information operators to trace their origins.

CHINESE INFORMATION WARFARE TERMINOLOGY

xinxi zhanzheng—information warfare

junshi geming—revolution in military affairs (RMA)

zhixinxiquan—information dominance

yitihua—integration

feixianxing zuozhan—seamless operations

zongshen zuozhan—deep strike

turanxing yu kuaisuxing zuozhan—sudden and quick strikes

dianxue—vital points

yuanzhan—over-the-horizon warfare

bingdu—viruses

wangluohua—networkization

xinxihua—informationization

feixianxing zuozhan—"a war without a front line"

zhiming daji—mortal strikes

xinxi gaosu gonglu—"information superhighway"

ruan shashang—soft destruction

kuayue—leapfrogging