Chinese Views on Information Warfare

By

Kate Farris

Naval War College,
Joint Maritime Operations
Prof. Ray Mach

2 April 2000
Information Cut off Date: 2/28/00

"In the near future, information warfare will control the form and future of War"

--- Maj. Gen. W. Pufeng
Former Director, Strategy Dept.
Academy of Military Sciences
Beijing

"Trying to know all about an adversary while keeping it from knowing much about oneself. It means turning the balance of information and knowledge' in one's favor, especially if balance of forces it not." Toffler

Kathleen Farris 5/16/00

REPORT DOCUMENTATION PAGE

1. Report Security Classification:	Unclassified
2. Security Classification Authority:	
3. Declassification/Downgrading Schedule:	
4. Distribution/Availability of Report:	DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.
5. Name of Performing Organization:	Dean of Academics Office
6. Office Symbol: 1	7. Address: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207
8. Title (Include Security Classification):	Chinese Views on Information Warfare
9. Personal Authors:	LCDR (s) Kati Farris
10. Type of Report: FINAL	11. Date of Report: 2/28/00
12. Page Count:	approx 50
13. Supplementary Notation:	A paper submitted to the Dean of Academics, Naval War College, for the DNI/DIA essay competition. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.
14. Ten key words that relate to your paper:	- Chinese Information Warfare - C4ISR - Six pillars of IW
15. Abstract:	Chinese views on IW are analysed in the context of the six pillars of IW.

16. Distribution / Availability of Abstract:	Unclassified	Same As Rpt	DTIC Users
17. Abstract Security Classification:	unclassified		
18. Name of Responsible Individual:	Dean of Academics, Naval War College		
19. Telephone: 841-2245		20. Office Symbol: 1	

"All men desire by nature to know"
Aristotle

Summary: As Aristotle said, "All men desire by nature to know." This is even more so in the military where people's lives hang in the balance of every decision. In order to make the correct decision in a timely manner, the key ingredient necessary is information. The military today is being driven to a more automated warfighting machine by the speed of warfare. This entails storage and retrieval of huge amounts of data, identification of threats, multiple offensive and defensive weapons systems, data sharing over wide areas, and split second decision on weapons release. Thus, more and more computer technology is being implemented. As such, a new group of offensive and defensive capabilities are requiring development so that our technological edge is not rendered helpless by fairly low-tech attacks on our interconnected military data networks.

Asymmetrical warfare has clear smart war features: Asymmetric warfare is grounded in the development of technology, particularly high technology ...Information or smart warfare has become the mainstay of asymmetrical warfare. The acquisition of accurate intelligence has always been a prerequisite for successful asymmetrical operations...Asymmetrical warfare is increasingly developing in the direction of no-contact warfare..Asymmetrical warfare will make the battlefield much more multidimensional.

- Jia Weidong,
Beijing Jiefangjun Bao
17 April 1999

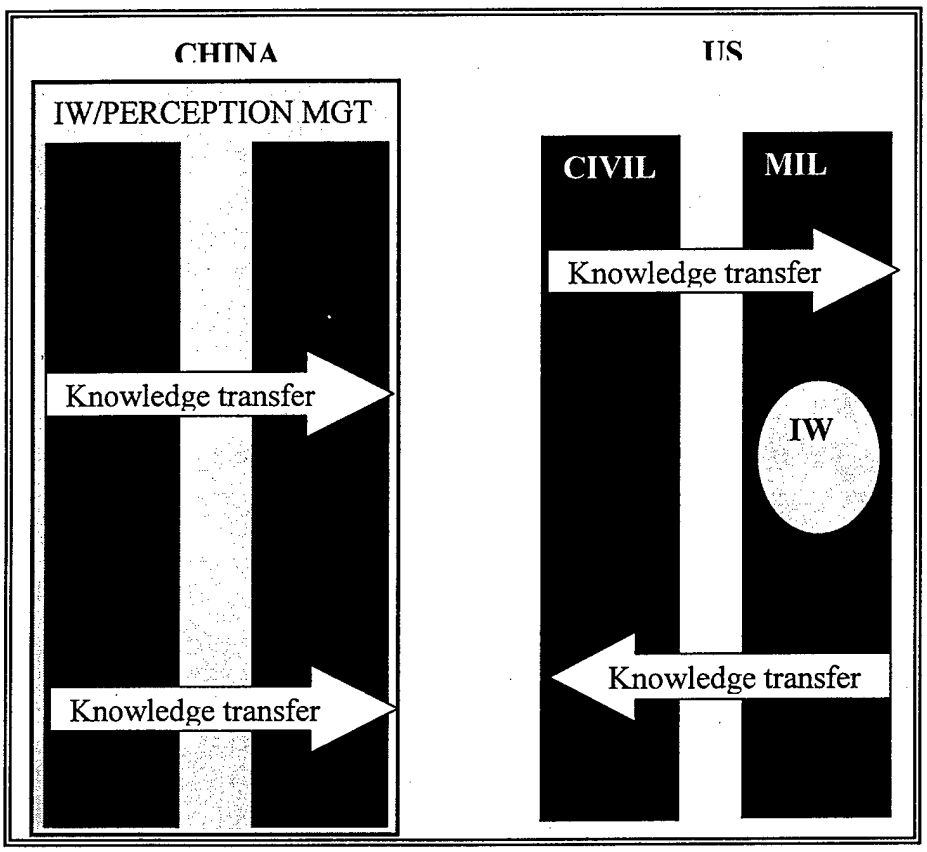
Although this paper addresses the Chinese view of Information Warfare, topics covered will be assessed in the US context of the Six Pillars of Information Warfare.[1] By using this context, it is readily apparent how different Chinese and US concepts are both in emphasis and focus of effort. These differences should be expected given the very different force structures of these two nations – and the corresponding inherent degree of incorporation of "high-technology" as the Chinese call it. But the roots of this difference go beyond just the military spheres. For China, IW, and its underlying premise of perception management, is a way of life in both the military and the civilian sectors.

China and the US also have a very different history of warfare. Since the writings of Sun Tsu in 500BC, Chinese military theorists have been advocating and practicing some of the concepts now incorporated into the theory of Information Warfare – psychological operations, camouflage/concealment and deception (aka

[1] US IO/IW definition of IW is found in Joint Publication 3-13, "Information Warfare is the wartime component to Information Operations, is a well-coordinated, national effort to achieve information superiority by affecting an adversary's information and information systems, with the intent or degrading the enemy's will or capability to fight."

Denial and Deception). They also have a plan to strengthen the areas they know are less well developed such as computer network defense.

It is clear from their unclassified writings that the PLA sees military utility in this information-based theory of warfare. Yet it would be incorrect to say that they are incorporating it into their new military doctrine. Local Warfare under High-Tech conditions, includes IW because IW precedes, overarches and encompasses all facets of military doctrine and strategy. It is all pervasive where non-combat tenets of IW are woven into combat strategy forming a unified whole. IW precedes conflict, and often continues after the conflict is over. The graphic below shows the differences between the Chinese and US approaches.



IW/Perception management envelops both the civilian and military sectors in Chinese life. It is a way of life. For the US, IW is found primarily in the military realm.

Transfer of knowledge recognizes that the IT revolution in the civilian sectors will lead those in the military. China anticipates taking advantage of this transfer. But the Chinese pre-occupation with security will preclude a more free flowing exchange of ideas as in the US.

The Chinese are institutionalizing IW by establishing civil and military institutions chartered to lead the PLA down the IW road to an operational capability that can be used from the national level down to the system level. As will be demonstrated, unlike their US counterparts, China sees IW mainly as an asymmetric tool – not the force multiplier the Americans see it as.

INTRODUCTION

Evidence of Chinese interest in IW is plentiful. Numerous journal and newspaper articles have appeared in various Chinese texts since the mid-1990s. These

discussions are not taking place in a vacuum. Appendix A outlines some of the major international and domestic events that shaped China's perceptions in the 1990s, including how they look at IW. In December 1999, an entire book was dedicated to IW. From this one source, it is readily apparent how different Chinese and US viewpoints are on this subject. The book, entitled *Introduction to IW* written by Dai Qingmin of the Electronic Engineering Academy.[2]

Evidence of China's value for IW is striking,

> "Beijing's development of information warfare is posing an increasing threat to Taiwan, Mainland Affairs Council (MAC) Vice Chairman Lin Chong warned on Monday. Lin, who is an expert on Beijing's military development, made the remarks at a ceremony marking the publication of his new book, titled "Nuclear Hegemony." *He predicted that information warfare ability will replace nuclear weapons at the top of Beijing's military development agenda for the next century.* Information warfare, or "acupuncture warfare" as Lin terms it, refers to the application of information or other high technologies to paralyze a nation's military command and control systems."[3]

One tenet that demonstrates how differently the Chinese view IW is found in how they incorporate this warfare tenet into a conflict whereby a "weaker power" can defeat a "superior adversary."[4] China has a long-standing tradition of claiming itself the "weaker state" that takes on a more powerful adversary and defeats him using asymmetric warfare. There is an ancient Chinese story that tells this story aptly from *Romance of the Three Kingdoms*.

Romance of the Three Kingdoms, is a story that describes a weaker army that has no arrows, and is about to face a very strong adversary, who has many arrows. A river separates the two armies. In the middle of the night before the battle, the weaker army floats several barges heaped with straw out into the middle of the river. When the next morning comes, and the stronger side sees these barges masking their view of the opponents' side of the river they are puzzled. Then the weaker army begins to thrash about in the water on their side of the river, but the stronger army can not see them because of these barges. The stronger army believes an attack is ensuing – even though they know they are the stronger power – and they begin firing their arrows into the air. There are actually few soldiers from the weaker army in the water causing all this raucous so the arrows tend to fall into the straw barges. This goes on for some time until the stronger army begins to question whether an attack was taking place or not, and they cease

---

[2] See Houqing, Wang, "Evaluating 'Introduction to Information Warfare'", *Jiefangjun Bao* 7 December 1999, as translated by Foreign Broadcast Information Service (FBIS) 7 December 1999.
[3] See Lee, Bear "Expert Warns Against PRC's Information Warfare", *Taiwan Central News* 31 May 1999, as translated by FBIS 5/31/99.
[4] See RAND 1999 "The US and a Rising China", www.rand.org/publications/MR/MR1082.html

firing. This cues the weaker army to float the barges down river, collect the arrows out of the straw and disseminate them to their own troops. Now the battle is a fair fight.[5]

Relative to the United States, China is well aware that her military's "high-technology" capabilities are far below that of the US[6] – thus, the US is considered China's potential "superior adversary".[7] Substantiating this position of a "weaker power", the Chinese have closely examined the lessons from Desert Shield/Desert Storm, and more recently Kosovo, and have attempted to upgrade the "high-technology" component of their military, but they know they are far behind the US in several critical technology areas.[8] They also recognize that as they incorporate some of these "high-technologies", it will cause reverberations throughout their entire military structure, rendering a "military revolution."[9]

> "China's military has a tradition of flexible fighting methods and is more adapted to nonlinear warfare, but it lacks practical battle experience in information warfare with high technology." [10]

> "Looking at the current situation, it can be seen that the authorized strength and equipment, strategy tactics, and military theory of PLA are still basically the products of the industrial era and are far from satisfying the demands of information warfare. We have much work to do to shrink this gap and our first task is to clarify our war preparation concepts. We have already made it clear that the basis of war preparation is to achieve victory in modern warfare, especially high-tech warfare and this is quite correct." [11]

With this background in mind, it is logical that China views IW quite differently from their US counterparts.

---

[5] See Lo Kuan Chung's *Romance of the Three Kingdoms*, translated by C.H. Brewitt Taylor, published by International Christian University, Tokyo, 1959. This story also demonstrates the Chinese emphasis of how superior tactics and strategy can overcome against a technologically stronger adversary. This theme will be repeated later in this paper.

[6] See Pillsbury, Michael, *Chinese Views of Future War*, National Defense University, Washington DC 1998. Also in Lilley/Shambaugh's *China's Military Faces the Future*, ME Sharpe 1999. In original reference, Pillsbury argues that "the PLA is preparing for asymmetrical warfare with a more powerful adversary (such as the United States) and acquiring the technologies and weapons systems to wage such a conflict." See page 5.

[7] Public debate in the US on this matter arose in 1996/1997 timeframe with the publication of the Monroe and Bernstein book *The Coming Conflict with China.*

[8] See "Taiwan's DPP Issues Defense White Paper", 23 November 1999. "In particular the revolutionary ideas regarding warfare since the Gulf War have a strong impact on the military thinking of the Chinese leaders."

[9] See Maj. Gen. W. Pufeng, former Director the Strategy Dept, Academy of Military Sciences, Beijing, in Pillsbury Michael, *Chinese Views of Future War*, National Defense University, Washington DC 1998p326

[10] ibid p324.

[11] ibid, p318.

One reference summarized the work to be done to realize IW's potential. They speak of the need to flatten and automate, command structures; systems architecture research (specifically system development and implementation, and operation); linking IW to increases in combat effectiveness; training personnel in IT use in warfare, and building both an intranet and an "extranet" which will be used solely by the military.[12]

The Chinese speak of different approaches to resolving these technological deficiencies, of which IW is only one of many deficiencies. Some, argue that the Chinese must adopt a symmetric response, and undertake the same pursuit of "high-technology" in as many aspects of their military a possible. Most however, argue for an asymmetric response[13], citing the fall of the former Soviet Union as an example of what can happen to a "weaker" country who attempts to match the US stride for stride.[14] Even for those who suggest a more symmetric response, that response will be with distinctly Chinese characteristics.

> "In the final analysis information warfare is conducted by people. The basic great plan is to cultivate talented people suited to information warfare...Talented information science and technology personnel are the pioneers of science and technology research..."[15]

This emphasis on people reminds one of the military doctrine of Peoples' War that existed under Mao. This doctrine envisioned that China would use her great geographic scope and large population to endure massed attrition along the country's periphery while drawing the enemy into the countries' interior where enemy supply lines would be overextended and severed.[16] This ability to absorb mass casualties, and conversely, the US unwillingness to do so, will be re-examined in the last section of this paper that discusses a potential China-Taiwan conflict.

When the Chinese argue a more symmetric responses, it is difficult to assess whether they truly support this view, or are simply parroting back what the Chinese are reading in the US press, and merely discussing US concepts without applying them to China. For example,

---

[12] See Prof. Chen Taiyi, Beijing *Zhongguo Dianzi Bao* [China Electronics News], 15 Sept. 1997 p 8, as translated by FBIS 10/24/97.

[13] See Pillsbury, Michael, *Chinese Views of Future War*, National Defense University, Washington DC 1998 page 5.

[14] Another reference states "The PLA can live with fewer resources because it saw what happened to the Soviet Union (total collapse), when Moscow tried to beat the West in an arms race." See Wortzel, *China's Military Potential*, Strategic Studies Institute, US Army War college, Carlisle PA, Oct 2 1998 (Carlisle-www.army.mil/usassi/ssipubs/pubs98/chinamil/chinami.html)

[15] See Maj. Gen. W. Pufeng, former Director the Strategy Dept, Academy of Military Sciences, Beijing, Pillsbury Michael, *Chinese Views of Future War*, National Defense University, Washington DC 1998 p325

[16] See Lilley/Shambaugh's *China's Military Faces the Future*, ME Sharpe 1999.

> "...From studies of foreign armies, we do not see any academic works which systematically discuss command and control in information warfare and technology in information warfare. Although our army has launched a number of research achievements, most of them are studies of foreign armies and *bear little reference to the existing conditions in our army.*" [17]

In a June 20, 1995 article in the Liberation Army Daily (*Jiefangjun Bao*), Senior Col. Wang Baocun and Li Fei state that,

> "Although military officials of all countries have not yet defined IW authoritatively, military experts in many countries have delimited its implications. While such definitions may be imperfect and even somewhat biased, they are certainly of great benefit to our understanding of the innate features of IW."[18]

Thus, the analyst must discriminate between Chinese reviews of US concepts and application of these concepts to the PLA (and any modification thereof). The context of the Six Pillars of IW, provide a simple methodology for sorting through this question. Once these distinctions are made, the next logical step is to test the hypothesis by evaluating the implementation of these uniquely Chinese IW tenets. Thus, a cursory examination of how the Chinese say they will get *From here* – today's military force structure and warfighting doctrine, *to There* - to tomorrow's military, and the steps taken to institutionalize IW within the PLA is appropriate and will be addressed in the latter half of this paper.[19] The last section of the paper will examine an IW case study – the current PRC-Taiwan crisis, and how the PRC is using IW in this crisis period. First however, a common understanding of what the Chinese define IW to be is necessary.

DEFINITION OF INFORMATION WARFARE

In a 5 November 1999 translation of an article that appeared in the *Tokyo Sankei Shimbum* press, a Taiwanese Air Force Officer was asked "What kind of war is 'information warfare'?" His answer was,

---

[17] See Yuanshen, Lei, "New Breakthrough in Study of Information Warfare", *Jiefangjun Bao* 21 Jul 1998, as translated by FBIS 7/21/98. Article discusses: "Command and Control in Information Warfare" and "Technology in Information Warfare" edited by Si Laiyi, Commandant of the Communications Command Academy, were recently published by the Liberation Army Publishing House. See too Zheng Wang, and Jianbo, Ke "IW: An Epoch Making Revolution in Warfare" *Chengju Dianzi Keji Daxue Xuebao*, December 1998 as translated by FBIS 12/01/98. This article provides a "tour de force" of worldwide IW interests and progress.

[18] Colonel Baocun then goes on to cite Lt. Gen. Cerjan, former President of National Defense University, writing in a 1994 Army Magazine article. See Sr. Col Baocun and Fei in Pillsbury Michael, *Chinese Views of Future War*, National Defense University, Washington DC 1998 p327

[19] A listing of these institutions are provided in Annex A.

> "Unlike the conventional warfare of using ranks, artillery, fighter planes and missiles to fight, this is a new type of warfare using electronic and computer technology to destroy or disrupt the information and communications systems, the military command structures, the state-run computer systems, and so forth of the enemy. In a broad sense, information warfare includes such things as waging a *psychological warfare* and manipulation of information to bring about social confusion or *paralyze the financial market*. It can also be regarded as a low-cost and highly effective means of fighting a war *without killing people*. The advanced nations with a high degree of dependency on computers will be highly vulnerable if they are not prepared."[20]

This last point is well illustrated by the concern that surrounded Y2K, and which fortunately, did not come to pass. *The Economist* put it another way, "Computer technology is now so ubiquitous that it is as important as safe drinking water and electricity."[21]

For comparison, a US IO/IW definition can be found in Joint Publication 3-13,

> "Information Warfare is the wartime component to Information Operations, is a well-coordinated, national effort to achieve information superiority by affecting an adversary's information and information systems, with the intent or degrading the enemy's will or capability to fight."[22]

In other words, it is actions taken to affect the adversary's information and information systems while defending one's own systems.

Chinese definitions build upon those of the US.

> "Chinese experts who are studying high-tech warfare have also defined information warfare thusly: Information warfare 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 other power to obtain, control, and use information. Information warfare is a combat aimed at seizing the

---

[20] Yajima, Seiji, "Taiwan Air Force Officer on Information Warfare with PRC". *Tikyo Sankei Shimbun*, 11/5/99, as translated by FBIS 11/6/99. Although a quote from a Taiwense officer, it is included here for its completeness and succinctness. PSYOPs, financial war will be discussed later in this paper. We will see its application particularly useful in the PRC's crises with Taiwan precisely because it permits warfare without Chinese killing Chinese – one of the key concerns of traditional warfare between PRC and Taiwan.

[21] See "Panic Postponed: Whatever happened to the Millennium Bug?" *Economist*, 1/8/00 p22

[22] Another reference, DoD 3600.1, July 1997, states "information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries."

battlefield initiative; with digitized units as its essential combat force; the seizure, control and use of information as its main substance; and all sorts of information weaponry [smart weapons] and systems as its major means. Information warfare is combat in the area of fire assault and operational command for information acquisition and anti-acquisition; for suppression [neutralization] and anti-neutralization; for deception and anti-deception; and for the destruction and anti-destruction of information and information sources.

We hold that information warfare has both narrow and broad meanings. Information warfare in the narrow sense refers to the US military's so called 'battlefield information warfare,' the crux of which is 'command and control warfare'...Information warfare in the broad sense refers to warfare dominated by information in which digitized units use information [smart] equipment... Information warfare in the broad sense has many manifestations as follows:

- Computer virus warfare. Sharven [as translated] claims that while the major 20th century weapons were tanks, the key 21st century weapon will be the computer...that will mean computer virus warfare...Some countries are now considering the organization and establishment of computer virus warfare platoons.
- Precision warfare. Precision warfare is characterized by less destruction and fewer casualties, less 'combat fog' and fewer troops, less logistics support and better troops mobility.
- Stealth warfare."[23]

Although these foregoing definitions of IW, be they Taiwanese, US or Chinese, sound very similar, their implementation will be very different. This can be seen in the next section where, using the six pillars of IW as outlined in US writings, it is easy to see which of these pillars China emphasizes. This emphasis is based on long standing historical strengths, and weaknesses they know require improvement. By definition, the type of military forces a nation has will impact the art of the possible in terms of information warfare possibilities. As was noted above by the Taiwanese Air Force Officer, "the advanced nations with a high degree of dependency on computers will be highly vulnerable if they are not prepared." He could have easily been speaking of the United States as it moves to a network centric environment, linking their high-tech Joint Forces across the battlefield, gaining information superiority and nearly omnipotent battlespace awareness -- at least as the objective. As he notes however, hopefully these same forces, will be prepared to continue functioning under conditions of IW. This

[23] See Senior Col. Wang Baocun an Li Fei, Pillsbury Michael, *Chinese Views of Future War*, National Defense University, Washington DC 1998 p318, 329-330. For additional References offering definitions of IW, see Pengqing, Li and Zhanjun Zhang "Explore Information Warfare Theories with PLA Characteristics" *Jiefangjun Bao* 11/24/98, as translated by FBIS 11/24/98.

focuses on what China calls "cyber war" or what the US calls computer network attack (C N A), which is only one of six pillars of IW.

Those nations who do not have the extensive dependency on layered information networks may be less susceptible to cyber war/C N A campaigns. China is quick to note that they have redundant land-line communication systems, or often use mere couriers to hand carry military orders back and forth even on today's battlefield. Plying successful C N A tactics against a more moderately technological force may be more of a challenge than against one that is absolutely dependent on maintaining control of the electromagnetic spectrum. Although lesser dependency may prove an advantage for the lesser developed country in a conflict, it traditionally has been difficult to parlay these minor advantages into an overall victory against a more superior power, and the Chinese have openly stated as much,

> "There is question of how to use weakness to defeat strength and how to conduct war against strong enemies in order to use information superiority to achieve greater victories at a small cost. It must be confirmed that information and weapons are all controlled by people. People are the main factor in combat power. However it must also be confirmed that the functions of people and weapons will primarily be determined by the control of information... In light of the fact that the military lags behind its strong enemies in information technology and information weapons, the military must emphasize the study of ways to use inferior equipment to achieve victory over enemies with superior equipment."[24]

Six Pillars of Information Warfare

Fundamental to many IW tenets is the concept of perception management. The ability to "manage" ones perception is the ability to get inside decision makers' decision cycles with the goal of influencing them. Perception management hinges upon what people perceive reality to be; regardless of what reality is. This perceived reality is what decision-makers base their decisions upon. Thus, it can be argued that IW tenets offer powerful means to influence perception management.

In US lexicon, IW has been organized in the six pillars of IW[25]

PSYOPS
Denial and Deception (D&D)

---

[24] See Maj. Gen. W. Pufeng, former Director the Strategy Dept, Academy of Military Sciences, Beijing, Pillsbury Michael, *Chinese Views of Future War*, National Defense University, Washington DC 1998 p318-319

[25] See Joint Publication 3-13.

EW
Computer Network Attack (C N A)
Physical Destruction
Operational Security (computer network defense [CND])

Using the six pillars context we will be able to readily assess the difference between Chinese and US views of IW. After this examination we'll review how the Chinese are moving IW, or what they call "no contact war", into realms for which the US has no corollary.

Before examining differences in these pillars, it is appropriate to briefly note a raging debate in the Chinese press over the applications of these no contact warfare means. It centers around fundamentally different approaches – that is indiscriminate attacks verses precision attacks. These approaches are at the heart of the debate on future warfare tactics. Both have merit, from the Chinese perspective, and both have costs associated with them. In the more traditional US military planning, the "precision" option inherently involves pursuing 'high-tech' means to achieve precision, yet China recognizes that this is precisely the area where China lags behind the Western technologies.

It is obvious from this debate that many questions remain as to how IW will be institutionalized in future military warfare doctrine and strategy. Although divided into six distinct pillars for analytical purposes, in practice, these pillars will overlap and complement one another (if done successfully), melding into a unified whole.

Pillar I - PSYOPS

Psychological operations (PSYOPS), denial and deception (aka camouflage, concealment and deception or CC&D), and other similar measures were the primary subject of one of the greatest military thinkers of all time, Sun Tsu, who wrote in 500BC. As evidence that his theories on warfare remain pertinent today, his primer *The Art of War*, is on the required reading list for many military academies, including those in the US.[26]

> Psychological Warfare: the planned use of propaganda and other psychological actions having the primary purpose of influencing the opinions, emotions attitudes and behavior of hostile foreign groups in such a way as to support the achievement of national objectives.
> Joint pub 1-02

> "To fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting." Sun Tzu

[26] This text is required reading for the Strategy and Policy Course taught at the Naval War College.

In essence, psyops uses perception management techniques to manipulate the enemy's decision making process.

One instrument of Psyops is propaganda. The US has always been suspicious of communist open literature, citing its propaganda content. Yet to most nations, propaganda need not be an outright lie, it's merely information dissemination that has its own agenda as its underlying purpose. The purpose is to get this agenda disseminated to the target audience. In modern US lexicon, this could be referred to as "spin." It is this definition that will be used herein.

By definition, current propaganda efforts often encompass media "war" as its transmission medium. One could view the 22 February 2000 publication of the "White Paper" on Taiwan as propaganda – the papers' stated purpose was to "further explain to the international community, the Chinese government's position and policy on adhering to the One China principle."[27]

It is true that some writings are almost solely meant to disseminate propaganda, and in their 1999 rift with Taiwan, the Chinese admitted as much in one article that discussed the "Second Stage of the PRC Propaganda offensive"[28].

> "It was understood that the first stage of propaganda offensives against Li Teng-Hui's 'two-state theory' had ended two days ago [19 July 1999]. The first stage focused on central-level media offensives against the 'two state theory'. On 25 July, the propaganda offensives will be extended to local media, while all local party and government organs, democratic parties, and non-governmental groups will declare their stand. At the third stage, there will be a wave of nationwide attacks against Li Teng-hui and the 'two state theory…' *the propaganda offensives are intended to make known China's position, educate its people and prepare public opinion for future possible military action.*"[29]

From this statement, we note that propaganda serves many purposes and therefore should not be dismissed out of hand. Propaganda can provide some clues to future enemy intent. True to their word, the Chinese conducted exercises in the Fujan Military Region beginning in August 1999, simulating, yet again, a mock invasion of Taiwan.[30]

---

[27] "White Paper on Taiwan" *China Daily,* 2/22/00, p4, as translated by FBIS 2/22/00

[28] See Kuo-Chung, Tsao, "Mainland's Propaganda Offensive Enters Second Stage", *Tai Yang Pao,* Hong Kong, 21 July 1999. As translated by FBIS 7/21/99

[29] See Kuo-Chung, Tsao, "Mainland's Propaganda Offensive Enters Second Stage", *Tai Yang Pao,* Hong Kong, 21 July 1999. As translated by FBIS 7/21/99

[30] The last large scale, highly publicized exercise was in March 1996. For an excellent summary and analysis of these events, see Garver, John *Face Off.* Some military analysts argue that these repeated military exercises off Taiwan may de-sensitize international response, specifically that of the US Seventh Fleet, so that if and when an attack is actually undertaken, it will encounter less initial resistance.

As is evident in the next lengthy quote, like IW, Psyops is all encompassing.

> "Scope of psychological warfare expands and its influence increases. As far as the scope is concerned, the psychological warfare in a local war in the future high-technology context goes beyond the confines of military struggle into political, economic, diplomatic, cultural, religious, and various other realms, forming an all-dimensional, highly in-depth, and multi-level operational effect. As far as the target is concerned, the main *aim is to strike and influence the enemy's decisionmaking stratum*, forcing it to waver in its position and make wrong decisions; the main task is to strike awe into the enemy's armed forces and upset their psychological equilibrium; the main approach is to cause terror in the general public of the other side, so that they will develop fear of war, war weariness, and opposition against war; an essential prerequisite is to obtain the sympathy and support of the international media and firm up the confidence in victory among the public of one's own country. In spatial terms, psychological warfare breaks down the boundaries between the front and the rear and between the theater of operations and the non-war zone. *In temporal terms, psychological warfare often takes place before the war and runs through the entire course of war, unfolding in all temporal and spatial sections, all domains, and all dimensions...*[31] The status of psychological warfare rises and its intensity increases. The *strategic status* of psychological warfare has been significantly raised, manifesting more as the application of strategic psychological warfare... The fully real-time diffusion via radio, broadcasting, and television through global satellites makes psychological warfare much more visual and time-sensitive... The means of psychological warfare is diversified and the striking force increases. The content of science and technology in psychological warfare has increased significantly. By using simulation technology, stealth technology, and camouflage technology to mix the spurious with the genuine, it is possible to cause psychological errors in the enemy, leading to errors in decisionmaking.... It is necessary to set up an organization for psychological warfare; form a theoretical system for modern psychological warfare with the characteristics of our Army, promulgate a training program for psychological warfare and regulations for psychological warfare operations, and standardize the training and combat of the whole

[31] See last section of this paper that discusses the information warfare that they have waged against Taiwan.

Army; set up specialized psychological warfare units; and strive to raise our Army's capabilities in psychological warfare."[32]

Pillar II - DENIAL AND DECEPTION (aka camouflage, concealment and deception)

Sun Tzu wrote:

> "All Warfare is based on deception. Therefore when capable, feign incapacity; when active, inactivity. When near, make it appear that you are far away; when far away that you are near. Offer the enemy bait to lure him; feign disorder and strike him. When he concentrates, prepare against him; where he is strong, avoid him. *Pretend inferiority and encourage his arrogance.* When he is united, divide him. Attack where he is unprepared; sally out when he does not expect you.[33]

Denying the enemy information he needs to reconnoiter, or attack you is the most basic form of denial. The Chinese have studied and written extensively on the Serbs success of denying US targeting information in the Kosovo conflict by executing simple, low-tech measures such as setting up smoke screens by burning rubber tires. Deceiving the enemy of your true capabilities and intentions by using denial, or concealing parts of your orders of battle is fundamental to the concepts of deception. Well-constructed camouflage nets can spoof electro optical (EO) sensors into not finding targets – or vice versa, well-constructed decoys can present an EO sensors with more targets than are really present.

In the section on Preparation and Defense with Attacking and Fighting, Gen. Pufeng assumes China will be on the defensive early in the campaign against a superior enemy, and denial and deception will be key to their success[34]

> "When China's enemies mainly use their air forces and navies to conduct strategic information warfare, China will be in the strategic position of defensive warfare along interior lines. The progress and outcome of the war will be determined by the state of China's advance preparations and defensive situation during the war....In addition to hiding and concealing forces, in combat, especially during key phases in key areas, we must engage even

---

[32] See Ping, Liu, "Military Forum" *Jiefangjun Bao* 18 August 1998, as translated by FBIS 8/18/98

[33] Sun Tzu, p66. The sentence in italics could be one reason the Chinese so readily accept and even publicize that they are the inferior power.

[34] In the section, *From here to there*, we will examine many means the Chinese discuss to win against a superior enemy. Some of these parables date back hundreds of years, such *as Romance of the Three Kingdoms.*

more actively in air defense warfare and intercept and attack enemy weapons as they arrive in surprise attacks." [35]

In a broader context, deception was combined with Psyops when Beijing failed to release to the Chinese public for four days, President Clinton's apology for accidentally bombing the Chinese embassy in Kosovo. Why would they use such deception? Perception Management among the Chinese population is extremely important. As mentioned in the introduction, perception management is routinely practiced in both the military and civil sectors, even in peacetime, although this is a particularly heavy-handed example of this practice.

ELECTRONIC WARFARE

When the concept of IW entered popular use, it had to be differentiated from that of an older, more venerable tenet, that of electronic warfare. IW could have been originally described as a greatly expanded EW concept.

Electronic Warfare

- Electronic Attack – denial of electromagnetic spectrum
- Electronic Protection – defense of electromagnetic spectrum
- Electronic Support – Gathering, analyzing reporting and storing electronic parameters and communications

- JCS Pub 1-02

For the Chinese, electronic warfare was a central node in the 1995 doctrinal shift away from Mao's peoples war to the concept of local war, where small and medium wars waged along China's periphery was the predominant threat after the fall of the Soviet Union in 1991. This effectively reduced the threat of strategic war, although did not eliminate it completely.[36]

Central to the evaluation and discussion of the new doctrine of Local War, was examination of the 1991 Gulf War by the US, and their allies. The Chinese were profoundly influenced by the events in this war[37], and lessons derived from it read like a wish list of a modern military.[38] Key among this list is the following,

> "Preparation for these three types of wars (small-scale conventional war, medium war, big war) shares some common requirements. These include developing precision guided munitions; cultivating modern military personnel; automating command, control communication and intelligence (C3I);

---

[35] See Maj. Gen. W. Pufeng, former Director the Strategy Dept, Academy of Military Sciences, Beijing, Pillsbury p321

[36] See Li Nan, "The PLA's Evolving Warfighting Doctrine, Strategy and Tactics, 1985-1995: A Chinese Perspective" in Shambaugh and Yang's *China's Military in Transition*, p184.

[37] See "Taiwan's DPP Issues Defense White Paper", 23 November 1999, as translated by FBIS 11/23/99.

[38] Li Nan, "The PLA's Evolving Warfighting Doctrine, Strategy and Tactics, 1985-1995: A Chinese Perspective" in Shambaugh and Yang's *China's Military in Transition* See page 193. .

enhancing *electronic warfare* capabilities; perfecting support and maintenance systems; reinforcing reserves."[39]

As with IW in general, EW is not just a wartime phenomenon,

> "In regard to the building up of EW weapons systems, one point that must be made is that peacetime and wartime efforts must be integrated. We must strive for quality and we must also amass a sufficient number of these systems. We can lay a good foundation for electronic support in wartime only if we persist in long term, uninterrupted surveillance during peacetime. We must gain a definite superiority in EW. The essential factor in achieving this superiority is to surpass the enemy in the number of information channels and in signal level densities within a specific range. Therefore, not having a sufficient quantity of equipment is unacceptable."[40]

One reference suggested the existence of specific EW "units" although it is a lone source.

> "The electronic warfare unit (shu zi wu qi), a new arm of the services which the outside world has been watching closely, has been established."[41]

Pillar IV - PHYSCIAL DESTRUCTION

Physical destruction is the most common warfighting tactic. Attrition warfare has existed for hundreds of years. However, when physical destruction is applied to IW, it focuses on destroying the information technology (IT) sectors of both military and perhaps civilian sectors – such as destroying national infrastructure sites. Some Chinese write of "decapitation" of key C2 nodes, or striking at the "links" in a network,

> "A combat system network comprising several scattered combat units could not operate without a relay or transformation function. As a network's connecting points are scattered and vulnerable to an attack, an enemy unit could easily attack and 'paralyze' them

---

[39] See Li Nan, "The PLA's Evolving Warfighting Doctrine, Strategy and Tactics, 1985-1995: A Chinese Perspective" in Shambaugh and Yang's *China's Military in Transition*, p184. It should be noted that although this resource document is extensive in its doctrinal discussions, it was written in 1997, just as the IW debate was heating up. For this reason, this concept is not discussed in Shambaugh and Yang.

[40] See Li Nengjing, Beijing *Zhongguo Dianzi Bao* [China Electronics News], 24 Oct 1997 p 8, as translated by FBIS 12/29/97

[41] See Liang Si., "Chinese Armed Forces are Increasing their Capacity for Fighting Electronic Information Warfare", *Zhongguo Tongxun She*, Hong Kong, 9 August 1999. As translated by FBIS 8/8/99

and thereby neutralize other combat system functions and throw a whole combat operation into passivity. In view of this, a future battle is likely to focus upon attacking, sabotaging, or infiltrating a *network's connecting points*; reducing each other's network efficiency...As a result a 'safe zone' in a traditional sense would turn into a 'sensitive zone' vulnerable to an attack along a blurred battle line between the front and rear; irregular 'war of nerves,' 'war of vulnerable point,' and 'war of vital parts' would replace a past 'carpet attack' launched at the outset; 'heartland attacks' or 'backyard attacks' would play a dynamic role at a combat stage from the start, thus making a battle highly unpredictable...Such a confrontation of one single solder 'pulling the emperor from the horse' is indeed an asymmetrical and unbalanced combat mode."[42]

"Conscientiously organizing *sabotage operations* by the Army, Navy and Air Force, grasp exploitable opportunities and make continuous raids to exhaust and wear down the enemy." [43]

"Information warfare includes engaging in an active offense of information suppression and attack, as well as in the reactive defense of information counter-reconnaissance, resistance to interference and defense against destruction ...we must strive for an *active approach* in a reactive situation and *use every means possible to destroy the opponents information superiority* and transform our inferior position in information. We must pay attention to...secret falsification, [which] can be used to plant false intelligence and false targets in the place of true intelligence and true targets to confuse the real and the false and muddle the opponents' perceptions and inspire false assessments. When conditions exist, *active methods* may be used to engage in interference to *blind or even destroy the opponents reconnaissance instruments*."[44]

Pillar V – COMPUTER NETWORK ATTACK

Of the six pillars of IW, Computer Network Attack (C N A) is what US analysts think of first when they think of IW. The Chinese often refer to C N A as "cyber warfare" or "Internet warfare". As will be seen in the *From here to there* section, the PLA has begun to incorporate simulated C N A, and its corollary, CND

---

[42] See Xihua Sun et al "No Victory Without Network in Future War" *Jiefangjun* Bao, 7/7/98, as translated by FBIS 7/7/98.

[43] See Maj. Gen. W. Pufeng, former Director the Strategy Dept, Academy of Military Sciences, Beijing, Pillsbury Michael, *Chinese Views of Future War*, National Defense University, Washington DC 1998 p324

[44] See Maj. Gen. W. Pufeng, former Director the Strategy Dept, Academy of Military Sciences, Beijing, Pillsbury Michael, *Chinese Views of Future War*, National Defense University, Washington DC 1998 p323

(computer network defense) into their exercises. This however, is not a sound approach to exercising the ability to continue to function in an IW environment specifically because the participants in the exercise have foreknowledge of an attack. One of the most difficult things in IW is the ability to definitively know whether or not you've been attacked, or if you have enduring problems for some other, more benign reason. Thus, these exercises, while indicative of an interest in continued functioning in IW environment, is not the best way to test such a case.

In an attempt to again differentiate between how the Chinese look at C N A and how the US does, this section will be divided into three subsections. The first, deals with the more traditional C N A familiar to Western analysts. The second examines how the Chinese intend to monitor what is said over the internet in order to detect any statements that might be traitorous to the state, and how they intend to control these statements. This is not C N A per se, but CNM – computer network monitoring, which could be a precursor to C N A. CNM is the concept of perception management being applied to civil sectors. This application has no parallel in the US. The last section looks at the problem of espionage. Although espionage could encompass all aspects of IW, it will be included in this section because fundamental to C N A is the concept of information attack, and information is at the heart of espionage.

Cyber War

September 1999, a month after the Chinese began annual exercises in the Fujan military region opposite Taiwan, an article appeared in the Hong Kong Press entitled "Taiwan Steps Up Training to Thwart PRC E-Warfare."

> "Several wargames held in China's Nanjing, Beijing and Lanzhou military districts since 1985 have focused on using electronic equipment to paralyze or destroy enemy computer and communications systems...Last month, Chinese computer hackers launched a *cyber war* to destroy the websites of several Taiwan government agencies venting their anger at Taiwan President Lee Teng-hui's provocative claim that the islands' relations with Beijing were 'state to state.' Local hackers fought back posting Taiwan's national anthem and national flag on several Chinese Government Agency websites. 'Although the attacks by hackers did not ruin information systems here in sectors such as banking and stock market, the effect of the scare on the public might be far-reaching,' warned Gen. Tang Yao-ming, Chief of the General Staff [of Taiwan]. 'We have to be cautious and should regard such events as the beginning of a potential electronic warfare,' Tang said."[45]

[45] "Taiwan Steps Up Training to Thwart PRC E-Warfare" *Hong Kong AFP* 14 Sept 1999, as translated by FBIS 9/14/99.

As can be seen from this quote, and as with all IW tenets, C N A must be preceded by extensive peacetime research and analysis to identify significant nodes.

Another article that discussed Internet warfare prospects appeared in *Jiefangjun Bao* on 11 November 1999.[46] This article suggests that a special "net force" will likely be established as a separate military branch. If this suggestion is correct, this concept differs completely from US concepts of IW, where within each service, this concept is embedded, as well as in the supporting C4ISR structures. It identifies three types of net warfare:

> "...information paralyzing software, information blocking software and information deception software. Some of these are like bombs, they are electronic bombs which saturate the enemy's cyberspace; some are like paintings, they are electronic scrawls which appear and disappear on the enemy's pages in chaotic fashion; some are like phantoms and electronic flying saucers which come and go on the net and disrupt the enemy's systems; it is also possible to develop masquerade technology to steal the internet power."[47]

Thus, these authors argue for developing software to resolve three problems.

> "The first is an electronic shield for warding off attacks from outside; the second is an electronic gate for preventing internal leaks; and the third is an electronic military policeman for blocking arbitrary actions. In addition, there is also recovery technology for heading off a disaster...it can still happen that part of the net will be sabotaged when attacked, so it is necessary to have corresponding software for net recovery."[48]

"Policing" the internet looking for anti-state positions (ie., CNM) may be a first step toward blocking these "arbitrary actions."

A subset of cyber war is information attack. To differentiate between information attack and physical destruction, the former would include measures that have already been discussed, such as seeding what the enemy believes to be a functioning network, with bad data. Usually, when the Chinese refer to the terms information attack, they mean infecting it with a computer virus, although as can

---

[46] Leng Bingling, Wang Yulin and Zhao Wenxiang, "Bringing the Internet Warfare into the Military System is of Equal Significance with Land, Sea and Air power", *Jiefangjun Bao*, 11 November 1999 p 7, as translated by FBIS 11/11/99

[47] ibid

[48] ibid

be seen in numerous writings including those of Maj. Gen. Pufeng[49] , this need not always be the case.[50] Predominantly, in the US lexicon the two are distinct.

Information attack is a broader approach to C NA. Information attack can be accomplished by massive information gathering and data correlation, both overt and covert, and often beginning in peacetime. An example of overt data collection would be using the Chinese nationals studying in the US as "poll takers" of US public opinions. Such data could be used to mislead the enemy in time of war, or depending on the data gathered, could be used to bolster Chinese military production based upon the information/technology gathered.

Big Brother is Watching

The Chinese have only begun the Orwellian monitoring of what is transmitted over the net. China feels threatened by the free exchange of ideas inherent in Internet transmissions[51], and has therefore begun forming centers that monitor what is transmitted, by whom, over what nets. Big Brother is alive and well in Beijing. Yet, the state fully recognizes the symbiotic relationship between civilian IT advances and the continued well being of the economy, which in turn, could support military applications.[52]

Although no one could argue that China today is far more progressive than even 20 years ago, some fundamental paranoia of the Maoist state prevails – the obsession to "control" free information exchange "could" challenge the legitimacy of the state. This paranoia manifests itself in a desire to control what is transmitted in internet forums. Yet how do you control the uncontrollable? It is (will be) the same problem Gorbachev dealt with after Glasnost (openness) started to take hold in Russia...how do you put the genie back in the bottle?

Under the heading, "China has engaged itself in an internet warfare and a special responsibility group has been set up to monitor public opinions on the Net" Chinese authors describe official Chinese policy to monitor what is said on internet chat rooms.

> "At the time when China and the United States were advancing towards a bilateral agreement on China's accession to the WTO, the CPC [Chinese Communist Party] had already taken active steps to find ways for countering the possible impacts that the entry of

---

[49] See Maj. Gen. Pufeng, in Pillsbury Michael, *Chinese Views of Future War*, National Defense University, Washington DC 1998 p322

[50] Bingling, Leng, Wang Yulin and Zhao Wenxiang, "Bringing the Internet Warfare into the Military System is of Equal Significance with Land, Sea and Air power", Jiefangjun Bao, 11 November 1999 p 7, as translated by FBIS 11/11/99

[51] See Lam Wo-Lap, "State Said Facing Losing Battle to Control Internet" *South China Morning Post* Hong Kong, 13 Sept 1999 p9 as translated by FBIS 9/13/99

[52] See for example, See Yaping Jiang et al "Zou Jiahua on Role of Information" *Beijing Xhinhua* 18 April 1997, as translated by FBIS 4/18/97

> foreign capital might exert on China's telecommunications industry, as well as ways for tightening its control over the spread of information. A special group has been recently set up, responsible for the anti-peaceful evolution [sic] work on the Internet. This special responsibility group is led by the Ministry of Public Security, and is composed of people from both the Ministry of State Security and the Commission of Science, Technology and Industry for National Defense...According to the source... the authorities have already recruited more than 2,000 computer professionals from different provinces across the country to monitor the public opinions on the net round the clock...The CPC authorities is learned (sic) to have set harsher internal rules for mainland electronic network providers during a recent period concerning the supervision and control of public opinions on the net...a network provider will be fined, suspended or even arrested and prosecuted for criminal liabilities if any of its much participated net forums, such as the Xinlangwang, Souhu, and Sitong is found to have carried remarks that may endanger the socialist country. What is more, the CPC has also drawn up a policy to empower its telecommunications industry to hit out on its own initiative. Under this policy, Chinese consortiums as well as overseas pro-CPC Chinese financial groups are encouraged and supported to take over large foreign telecommunications companies, with a view to bringing under control 'sources of infiltration' outside the country."[53]

Espionage

In the Fall of 1999, relations between the US and China seemed at its lowest since the 1995 publication of the Ross Munro book "*The Coming Conflict with China*" that basically claimed the PRC was to be the next "evil empire"[54]. Events that fall were: the vehement rhetoric between China and Taiwan over Lee's July 1999 "state to state" comment, the May 7 accidental bombing of the Chinese Embassy in Kosovo[55], the missed opportunity of PRC acceptance into the WTO,[56] and release of the "House Select Committee on US National Security and

---

[53] See Su-li Wu "Shenzhou Space Strategy", *Hong Kong Kai Fang*, 5 December 1999, as translated by FBIS 5 December 1999

[54] During this period Sino-Russo relations were surging forward in a "strategic partnership." See Bin, Yu, "Sino-Russian Relations: Nato's Unintended Consequence: A Deeper Strategic Partnership...or More" " in the July 1999 CSIS *Comparative Connections*.

[55] See Gates, Robert, In War, Mistakes Happen, *New York Times,* OP-ED page, 5/12/99

[56] The PRC reached agreement with the US over WTO conditions in December 1999, after much protest at the Seattle Washington meeting. This note references the previous attempt to discuss this matter in April 1999, when Premier Zhu Rongju visited the US and offered unprecedented concessions, which the Clinton administration rebuffed. For an excellent summary of the April 1999 discussions, see Glaser, "US-China Relations: Challenged by New Crises" in the July 1999 CSIS *Comparative Connections*.

Military/Commercial Concerns with the People's Republic of China" report, better known as the Cox Committee report. This report concluded that China,

> "Stole design secrets on the US's most advanced thermonuclear weapons and used them to help develop miniaturized warheads; stole US missile guidance technology with direct applications for China's ballistic missiles, including short-range missiles and ICBMs; and stole US missile guidance technology that has direct applicability to its ballistic missiles and rockets... the report concluded that China now possess both the capability and intent to build a nuclear arsenal on par with that of the US and forecasted the deployment by China of 1,000 warheads atop land-based ICBMs within 15 years."[57]

This references' author, Ms. Glaser, argued that many of the allegations in the Cox report were unproven at the time of its publication, and the object of the report, a Chinese scientist working at Sandia's National Lab, was not formally charged with any wrong doing until December. This report was used by critics of the US "engagement policy, ".[58]

China openly admits that many of the visiting scientists, students and other Chinese nationals living in the West collect unclassified data. Many are even used to pulse public perceptions to differentiate them from that of the Western governments. But one wonders what the bureaucracy back in Beijing must be like to read all these inputs and coordinate this information.

Pillar VI – OPERATIONAL SECURITY (CND)

The US concept of CND is only now coming to the forefront of Chinese efforts. Although they recognize the dialectic – which should ensure that CND is pursued as actively as C N A, there has however, been very little written in the Chinese open press about CND. There is one reference to advancements in encryption codes. Beyond this, they wrote of military exercises held since 1997 that focused on combating computer viruses, so even though they're not talking about CND per se, it seems they are working on it. This may suggest that the Chinese feel they are particularly vulnerable

> Information Security: A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: identify those actions that can be observed by adversary intelligence systems; determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; select and execute measures that eliminate or reduce friendly actions to adversary exploitation.
>
> JCS Pub 1-02

[57] Glaser, "US-China Relations: Challenged by New Crises" in the July 1999 CSIS *Comparative Connections*. See too Summary of the Cox report on www.cnn.com/ ALLPOLITICS/resources /1999/cox.report/overview.

[58] See Tyler, Patrick *A Great Wall: Six Presidents and China*, Century Foundation, New York, New York1999

in this area. A review of the military exercises will be offered in the *From Here to There* section of this paper.

The more traditional operational security measures of OPSEC, D&D, and PSYOPs, have already been reviewed and the Chinese are very strong in some of these more traditional areas. CND can be aided by these traditional strengths, but alone, they will not guarantee CND. The most direct form of CND is sophisticated encryption devices.

> "Information encryption: Information encryption is a better solution against network wiretapping. An information identification mechanism should also be introduced to prevent IP deception. The American Data Encryption Standard (DES) is the most well known method of encryption that utilizes 56-digit key. It performs at least 16 complex iterative replacements and transmission processes for data encryption. However, the reliability of the DES encryption technique is not very high... Additionally, there are many shared keys that need to be controlled in a large network system. Hence, this design does not have great practical value. The problem of key management can be circumvented by public key encryption (PKE). Since it requires 100 million years to do the calculations involved in the decomposition of a large number N (the digit number of the information) to the multiplicity of two prime numbers, a PKE system is very safe and the information possesses high corruption resistance. Its decoding requires a special key. Distribution and transmission of a special key can be handled by a combination of public and private keys." [59]

"The general is skillful in attack whose opponent does not know what to defend; and he is skillful in defense whose opponent does not know what to attack" Sun Tzu

Having demonstrated how different Chinese views of IW are contained within the Six IW Pillars, this next section reviews the new realms in which China is pushing IW. These realms have no corollary in the US.

---

[59] See Binghua, Liu, "Technical Attacks on Network Information Systems, Security Countermeasures" *Beijing Zhongguo Guofgang Keji Xinxi* (Chinese Defense Science and Technology Information), June 1997, as translated by FBIS 6/1/97

Chinese Expansion of IW concepts

> "Author Shen Weiguang is a foregoer of the information warfare science in our country. He released an article on the theory of structural information warfare in 1987 and published a book entitled *Information Warfare* in 1990, signifying that the Chinese research on information warfare has joined the forefront of the world. In September of last year [1998], Shen Weiguang attended the first international forum on information warfare held in Austria. In his speech, he appealed for 'checking information warfare,' which caught the attention of the world. Just as the purpose of China's possession of nuclear weapons is to end the nuclear monopoly and stop nuclear wars, the purpose of China's research on information warfare is to prevent this new war monster from havocking mankind and create an international safety environment favorable to peace and development. Only when we possess the capability to win, and make preparation to win, can we possibly realize the aim of checking the warfare."[60]

The Chinese have advanced IW/"no-contact warfare" concepts into arenas that have no parallel in the US. The best example of this is provided in the book *Unrestricted Warfare*. This book spans all six pillars of IW as well as outlines these new applications. For this reason the book will be addressed here rather than separately under each pillar. This book is also a good source to understand how Chinese analysts say they should asymmetrically respond to the challenges put forth by the US "high technology" military.

Unrestricted Warfare, by Qiao Liang, and Wang Xiangsui

Perhaps one of the more well known Chinese publications on"no-contact warfare", is the February 1999 book entitled *Unrestricted Warfare: Assumptions on War and Tactics in the Age of Globalization.* The book was published by the PLA Literature Arts Publishing House. The authors, are both senior colonels in the PLA Air Force (PLA-AF), who, according to their unclassified biographical data, participated in the March 1996 exercises against Taiwan.[61] During an interview with Qiao Liang, on 19 September 1999 by the *Hong Kong Ta Kung Pao* (a PRC owned newspaper in Hong Kong), Liang was asked what inspired him to write this book. His response,

> "The military exercises in the Taiwan Strait in 1996 are the immediate cause for writing this book." [62]

---

[60] See Weiguang Shen, "Checking Information Warfare..." *Jiefangjun Bao* 2/2/99 p6, as translated by FBIS 2/2/99

[61] These exercises were the largest scale against Taiwan by the PLA since Taiwan's inception.

[62] See Ling, Ma "Author Discusses 'Unrestricted War' Book", *Hong Kong Ta Kung Pao*, 19 September 1999. As translated by FBIS 9/19/99.

Liang and Xiangsui were strongly criticized in the western press when this book came out. Western analysts claimed the two were advocating the adoption of guerilla warfare/terrorist tactics, particularly in the thinly veiled war of a weaker power against a stronger – such as China against the United States.[63]

During the interview, Liang outlined how the nature of war has "generalized" to encompass many facets heretofore not recognized as part of warfare. He discussed something he calls "dislocation methods", which

> "...completely upsets the order of the cards in ones own hands and reorganizes them in accordance with the needs of war and interests by that time... Here the train of thought is endless and there is a great variety of applicable means. For example, applicable military war methods include atomic warfare, conventional warfare, biological and chemical warfare, ecological warfare, space warfare, electronic warfare, guerilla warfare, and terrorist warfare; applicable *above-military war methods* include diplomatic warfare, network warfare, technological warfare, smuggling warfare, drug warfare, and fictitious warfare (deterrence), and applicable *non-military war methods* include financial warfare, trade warfare, resources warfare, economic aid warfare, legal warfare, sanction warfare, media warfare, and ideological warfare."[64]

One can see from this quote, that the Chinese concepts of IW cut across "*applicable methods...above-military methods...and non-military methods*" of warfare. Relating back to the Six Pillars of Information Warfare, it is easily discernable that the following are emphasized: electronic warfare; network warfare (i.e., computer network attack); psychological warfare; ideological warfare (no pillar corollary, but related to perception management)

To return to Liang's interview, he advocated a "generalization of warfare" by combining the various "*applicable methods...above-military methods...and non-military methods*" of warfare so that the weaker country might be able to defeat the stronger one. This is an example of a classic asymmetric strategy.

---

[63] Ibid. During the interview, Liang is asked whether he thought he was advocating "spreading terrorism." "Can such actions as terrorist activities, hacking, financial attacks and drug trafficking be considered war?" his interviewer Ma Ling asked (p3). His response, "since the Americans are already doing it, why can't we discuss it?" Liang sites US attacks against Iraq, Yugoslavia and Bin Laden as evidence. "(these attacks) were no longer using purely military means. Its media war, news restriction, trade sanctions and such financial attacks as freezing the other party's assets all took place simultaneously with the war actions and were used more thoroughly than any country." (p4)

[64] Ibid. page 3

These measures take the term "war" to its most encompassing description and assigns it to such concepts as "financial/economic war," and "media war" among others. It stands in stark contrast to US reticence to call anything "war."

In his book entitled *Face Off*, where author John Garver chronicles the US-Sino-Taiwanese crises since 1996, he notes that in anticipation of such an electronic threat to Taiwan's banking and financial markets, extensive monies were moved out of the Taiwanese markets. He also charges that Beijing deliberately led Taiwan to believe there would be an EW attack, in the hopes of provoking an economic panic against the Lee government.[65]

> "For Soros, another infamous figure, no-limit warfare also finds favor, because in the modern world, financial terrorism (a new term created by Qiao Liang) is terrifying, being capable of launching a destructive strike on a country's economy in just a few days, to affect targets all the way from the state central bank to the common man. The financial crisis that started two years ago and nearly destroyed half of the world was a 'one-man war' by Soros, with Hong Kong's prosperity nearly being destroyed by him alone. If it had not been for Chinese Government backing, and if the Chinese Government had not kept the renminbi [RMB] from being devalued, to keep a certain order, the financial crisis would have spread to the United States, with Wall Street being one of its victims. So if the world really does not know what to do, leaving such big financial fish with such power, they will hold up the whole world. *The Los Angeles Times* ran an article in August 1998 saying that "the greatest current threat to the world is the financial market, not terrorist training camps."[66]

Making no judgement on the validity of these charges, this is a good example of what the Chinese consider to be financial warfare. They rightly note that the United States pressured Beijing heavily not to devalue the renminbi during the Asian crisis, which would certainly have been in their own best interests to do. But as the article notes, that action would have sent the shock waves of the Asian financial crisis even deeper into the world financial markets. It would seem that under financial war, they would like to be able to assess just how far and to what extent these shockwaves would occur.[67]

---

[65] See Garver, John, *Face Off China, the United States and Taiwan's Democratization,* University of Washington Press, page 125.

[66] See Lin Sha, "To Senior Colonels and 'No-Limit Warfare'", *Beijing Zhongguo Qinnian Bao,* 28 June 1999, as translated by FBIS 6/28/99. George Soros heads the Soros Foundation, a philanthropic organization that was instrumental in establishing loans for former Soviet bloc stated. For more on the Soros Foundation, see www.Soros.org.

[67] See Bingling, Leng, Wang Yulin and Zhao Wenxiang, "Bringing the Internet Warfare into the Military System is of Equal Significance with Land, Sea and Air power", Jiefangjun Bao, 11 November 1999 p 7, as translated by FBIS 11/11/99 for Fighting 'No-Contact Warfare' – On the

> "National economic security is facing more rigorous challenges... Greater the interdependency, bigger the threats... If the enemy country applies the means of networking crimes in an organized and purposeful way to conduct economic interference and obstruction, it would collapse the economy of the country concerned. Some data indicate, at the present time some countries are studying and developing "super viruses" and electromagnetic devices which can, when necessary launch attacks on the banking, stocks exchange, air traffic control, telephone, TV, power stations, and electric power systems of the country concerned to paralyze its economy." [68]

As was mentioned previously, IW can be waged at the national, operational and tactical/systems level. The national level would focus perhaps on nations' infrastructure. Such a target would be strategic in nature.

> "Strategic information warfare has already started in the peaceful environment and has been manifested as intelligence war and propaganda war. Potential threat will come more from information space."[69]

But one preeminent Chinese author noted that all these efforts are steps in a lengthy process toward a goal called IW.

> "Information warfare and informationized war have both similarity and difference. Their similarity is that in both information warfare and informationized war, information plays a dominant role and matter and energy play a secondary role; the difference is that information warfare is a format of fighting and part of a complete war, but informationized war is an all-new form of war. The connection between the two is that as time goes by, the connotation of information warfare will gradually expand and eventually develop into informationized war... It is estimated that informationized war will not come into being until Western countries set up informationized forces by the middle of the 21st century."[70]

Need to Focus Our Preparations for Military Struggles", *Beijing Jiefangjun Bao* (Internet Version), 4 October 1999, as translated by FBIS 4 October 1999

[68] See Weiguang Shen, "Checking Information Warfare..." *Jiefangjun Bao* 2/2/99 p6, as translated by FBIS 2/2/99

[69] See Jianghuai Wang and Dong Lin "Viewing our Army's Quality Building form the Perspective of What Information Warfare Demands" *Jiefangjun Bao* 3/3/98. As translated by FBIS 3/3/98

[70] See Baocun, Wang "New Military Revolution in World: Subdueing Enemy Forces without Battle and Informatized Warfare" *Zhongguo Junshi Kexue*, 5/4/99. As translated by FBIS 5/4/99

Chinese IW – From Here to There

Inherent in the debate on where the Chinese wish to take IW, is embedded the controversy of pursuing a symmetric vs asymmetric options. This embedded debate is important to understand because the outcome of this controversy will ripple through how they implement IW. An asymmetric focus would support "blanket" attacks. Those that are indiscriminate in nature – such as using Electromagnetic pulse weapons to neutralize all electronics within its lethal radius. The problem with this approach is the imprecision of expected outcome – if a critical target happens to be 3m outside the lethal radius, it may continue to function. A symmetric response would entail precision attacks, whereby extensive knowledge of the target system is required, but the outcome of the attack may be more readily assessed.

An article that appeared in the 11 November 1999 edition of *Jiefangjun Bao,* interprets things more narrowly and seeks a traditional cause and effect correlation of actions taken, than of indiscriminate attacks. In this particular case, topic matter is C N A or "cyber war" or "net warfare."

> "Both blind attack and blind defense in net warfare will not do. It will not do to launch a blind attack without regard for the degree of severity or urgency and still less can one launch an indiscriminate attack without regard for the effectiveness of the means employed: that is, there must be technology, tactics, and pursuit of actual effect...Experts concerned believe that net attacks have not yet been fully put to good use, because corresponding links have not been established between such attacks and combat actions, since each fits its own war. To ensure that net warfare can play the maximum role in war, it is essential to integrate it with other combat actions...nor can it be won just on the net."[71]

This article seems to be suggesting that any attempts at blanket attacks – such as electromagnetic pulse weapons that would indiscriminately blind all sensors within range of detonation – not be used.

The implications of these imbedded debates are significant. The US has taken great pains, and spent large sums of money to be able to accommodate the precision warfare used in Desert Shield/Desert Storm in 1991, Kosovo in '99 (accidental bombing of the Chinese Embassy excluded), and in Military Operations Other Than War (MOOTW) operations, such as the Tomahawk attacks on reported Bin Laden positions in Afghanistan. Such warfare dictates that we have near perfect situational awareness and the ability to do "smart

[71] See Bingling, Yulin and Wenxiang "Bringing Internet Warfare into the Miltiary System is of Equal Significance with Land, Sea and Air Power", *Jiefangjun Bao*, 11 November 1999. As translated by FBIS 11/11/99.

targeting" with our "smart weapons." The objective of such "smart targeting" is to minimize collateral damage to non-military targets. We have built an extensive system of intelligence support to provide the needed information for that precision and the extensive C4ISR net that ties it all together. Yet, for all these efforts, occasionally, we still fail – such was the mistaken bombing of the Chinese Embassy in Belgrade. If such precision is to be had, it comes at a great cost, both monetary and in terms of intelligence preparation of the battlefield. A much simpler solution is offered by those "blanket" attacks, and as the Chinese have often pointed out, collateral damage to one's own troops is minimized by definition, if those troops are not as dependent on the C4ISR assets blinded by the attack, as is the enemy.

> "Information advantage does not mean that information technology can determine the destiny of a country, and it is an irrefutable fact that countries in a position of 'information disadvantage' can produce some kind of 'asymmetrical advantage.'...Information advantage does not mean psychological or volitional advantage. To the contrary, it may prove 'counterproductive' "[72]

But as the dialectic continues opposing viewpoints are again expressed, advocating a more blanket approach.[73]

> "Moreover, the Chinese Communists have established a high-technology special force in the Guangzhou Military Region to carry out various types of information warfare. They also have begun to assess and experiment on the damages caused to electronic equipment of command and control centers by electromagnetic pulses generated by a nuclear explosion or an electromagnetic bomb. They have made initial progress in the development of tactical electromagnetic pulse weapons which do not cause nuclear radiation pollution."[74]

Having examined how the Chinese view IW differently from the US and the seemingly dual track of pursuing symmetric and asymmetric options, it is logical to examine how they've put those different viewpoints into practice and understand how these differences manifested themselves. The first part of this section will address this issue, and examine international purchases and indigenous R&D support for IW related programs – to include C4ISR programs, which underpin IW both offensively and defensively. The second part of *From Here to There* will look at institutionalizing IW. By creating institutions, China ensures IW is as much a part of their civil structures as it will be in their military.

---

[72] See Demin, Zhou, "Dialectic View of Information Advantages and Disadvantages" *Jiefangjun Bao*, 28 Apr 1998 p6, as translated by FBIS 4/28/98.
[73] "PRC. Taiwan Modern Warfare Viewed", *Chung-Yang Jih-Pao*, Internet Version, 11/22/99. As translated by FBIS 11/22/99.
[74] ibid

The last section will examine military exercises that include IW, or more recently, focus on IW.

Symmetric and Asymmetric IW Pursuits:

Now that we have reviewed the differences between US and Chinese IW concepts, and have seen that China knows they lag far behind the US in the breadth of high-tech weapons, do the Chinese write about how they intend to pursue IW in the future? Will they, like the days of the Cold War with the Soviet Union, take the bait and accept a symmetric response[75], or do they intend an asymmetric response?[76] From unclassified Chinese writings it is clear they intend to do both – pursuing the C4ISR network necessary to target precision weapons – but to also rely heavily on traditional asymmetric military tactics and strategy of Sun Tzu. Moreover, if one examines the latest rift between the PRC and Taiwan as a case study, it is clear the PRC is today pursuing both options in this case study.

Symmetric IW: Enhancing C4ISR Connectivity

In just the last few years, the PLA has made tremendous gains in C4ISR improvements. These improvements have application across all six pillars of IW and all facets of warfare in general. This has been quite an accomplishment addressing a heretofore serious shortfall.

In a review of doctrine, strategy and tactics from '85 to '95, author Li Nan notes the following shortfalls in modern air defense systems, as an example of a mission area intensive in C4ISR requirements.

> "...incorporating unified intelligence and early warning functions, and countermeasure systems; air combat arms capable of rapid reaction, night, all weather and ultra-low flying capabilities to support combined arms operations; long range transport assets; airborne refueling capabilities; offensive air capabilities capable of sustaining independent, massive, incessant, long period air raids; night vision technologies and hardware such as thermal imaging

[75] In Lilley/Shambaugh's *China's Military Faces the Future*, Paul Godwin's assessment of PLA capabilities in technology, doctrine, strategy and operation is that "while some significant advances have been made in the development of new doctrine and operational concepts, and some relatively recent vintage weapons platforms have been acquired from Russia, the PLA of today is still 30-40 years behind the state of the art across the board in most conventional capabilities." See page 4 Another reference, states "The PLA can live with fewer resources because it saw what happened to the Soviet Union (total collapse), when Moscow tried to beat the West in an arms race." Wortzel, Larry M. *China's Military Potential*, Strategic Studies Institute, US Army War College, Carlise PA, Oct 2, 1998.

[76] "...the PLA is preparing for asymmetrical warfare with a more powerful adversary (such as the United States) and acquiring the technologies and weapons systems to wage such a conflict." See Pillsbury, Michael, *Chinese Views of Future War*, National Defense University, Washington DC 1998 page 5

> systems for infantry and helicopters, and countermeasure systems; a C3I system that utilizes surveillance and navigation satellites, and integrates functions of reconnaissance and target acquisition, electronic data processing and relay, and countermeasure systems; precision guided munitions; and modern logistics." [77]

This list was written in 1997, as of late 1999, the Chinese were negotiating with Israel to obtain AEW aircraft; they have procured, incorporated, and will co-produce the FSU air superiority aircraft SU-27 FLANKER into the PLAAF, and announced that they were about to purchase the SU-30. Both the SU-27 and the SU-30 are all weather, night capable, refueling capable offensive air fighters. They successfully procured aerial refueling kits on the international market and in December 1999, they launched a navigation satellite. Additionally, Moscow announced that effective January 2000, when Defense Minister Chi Hotian visited Moscow as part of the expansion of Russo-Sino military technology exchanges, China would be granted access to the Russian GLONASS system, which, the Russians claim, permits targeting of ships at sea.

> "The presence of precision guidance technology is the key indicator of the sophistication of information modernization in munitions systems. The primary factors in precision guidance technology are the ability to acquire target information with a high degree of sensitivity and the ability to precisely determine the position of the target and track it. Thus, precision guidance technology really represents a high-tech integration of aerodynamics and information technology." [78]

The Chinese are also interested in "counters" to all these systems, paying homage to the Marxian concept of "negation of the negation" as it applies to the dialectic.

In addition to adding these various reconnaissance and surveillance platforms, the Chinese are creating the C4 structures necessary to wage modern, joint force combat.[79]

> "Chinese military technology experts stress that China should develop a characteristically Chinese military network and build a nerve system for future warfare. Before the ninth Five Year plan period ends [2002], Chinese armed forces will have improved the

---

[77] See See Li Nan, "The PLA's Evolving Warfighting Doctrine, Strategy and Tactics, 1985-1995: A Chinese Perspective" in Shambaugh and Yang's *China's Military in Transition*, p184. It should be noted that although this resource is extensive in its doctrinal discussions, the IW debate is not discussed in Shambaugh and Yang.

[78] See Li Nengjing, Beijing *Zhongguo Dianzi Bao* [China Electronics News], 24 Oct 1997 p 8, as translated by FBIS 12/29/97,

[79] See Liang Si., "Chinese Armed Forces are Increasing their Capacity for Fighting Electronic Information Warfare", *Zhongguo Tongxun She*, Hong Kong, 9 August 1999. As translated by FBIS 8/8/99

> functions and configurations of their military strategic communications network that have been built, and completed the transition of their technical system under which analogous operations will be replaced by digital operations, communications cables will be replaced by optical fibers, switching by space division [kong fen] will be replaced by program – controlled switching, communication network will be able to handle multiple tasks instead of single task, communications terminals will have multiple functions instead of one function, and artificial communications management will be replaced by automated management. Meanwhile, efforts are being made to speed up the building of supporting systems such as the digital synchronization networks, common circuit information networks [gong lu xin xi wang], intelligence networks, communications management networks and so forth. During the period from the 10th Five year Plan, through the year 2010, a network of defense information systems that has integrated broadband services, that supports mobile subscribers connections, that is safe and confidential and that is destruction and interference resistant will be basically built for the armed forces." [80]

Key among China's resources for their military buildup will be their continued access to Russian technologies, which could render the "swift return of the world to the Bipolar system."[81]

Symmetric IW: Knowledge Transfer from Civil Sectors

Even though, as was noted in the summary, China is behind the West in many IW technologies, they are not completely without resources. Those discussed in the open press primarily relate to capabilities that are found in the civilian sector, but it should be remembered that the synergy between the two sectors will facilitate information transfer into the military realm.

> "China already has capabilities to utilize existing mid to low speed information networks and build additional ones, as well as capabilities to do research on high-speed information networks and build them. Consider the following facts: 1) packet data communication networks already cover more than 20 large and mid-sized cities throughout all of China, and digital data backbone networks already cover 3 municipalities that are directly under the

[80] See Liang Si., "Chinese Armed Forces are Increasing their Capacity for Fighting Electronic Information Warfare", *Zhongguo Tongxun She*, Hong Kong, 9 August 1999. As translated by FBIS 8/8/99

[81] Bin, Yu, "Sino-Russian Relations: NATO's Unintended Consequence: A deeper Strategic Partnership...or more", *Pacific Forum CSIS, Comparative Connections*, A Quarterly E-Journal on East Asian Bilateral Relations, Vol I, Issue I July 1999. See also, Glaser, Bonnie S, "US-China Relations: Challenged by New Crises", ibid.

authority of the central government as well as 21 cities that are provincial capitals. 2) Some optical cable trunk lines, digital microwave trunk lines and large and mid-sized satellite communication earth stations were built during the Eighth FYP. During the Ninth FYP, a network of eight horizontal and eight vertical optical cable trunk lines will be built that will cover all of the large and mid-sized cities throughout all of China.3) Domestic computer data communications networks are already distributed among large and mid-sized cities throughout all of China. Some of these networks can communication information such as email, data related to management and scientific and technical data. Moreover some of these networks are connected to the Internet. The 'Three Golden Projects' are now in the process of being built. 4) Historic strides have been made in the development of China's posts and telecommunications switches in China's urban and rural areas already makes this one of the largest telecommunications networks in the world."[82]

"Faced with worldwide competition in the information sector and the challenges posed by IT, the task of building an information age China should proceed in a planned fashion in accordance with the points outlined below:
1. Build an information network architecture suitable for use by the civilian and military sectors in peacetime and wartime. IT is a factor that has a multiplier effect on the growth of the national economy...2. Strengthen the training of capable people. The existence of advanced IT is dependent on having people who can understand it. 3. Give free rein to the market's driving power. China's 'three networks' have already begun to take shape: they are 'the Public Communications Network', the 'Economic Information Network', and the China Education and Research Network (CERNET).' 4. Adopt new technology 5. Enhance the survivability of information networks...The information flow command and controls the flow of personnel, material and energy resources. Hence the bright prospects for IW characterized by 'soft kill' procedures that are flexible and varied. 6. Strengthen legislation concerning information and strengthen information administration... INFOSEC is an important mainstay of national defense and safeguard of national security."[83]

[82] Wang Xusheng, Su Jinhai and Zhang Hong, PLA Academy of Electronic Technology, *Jisuanji Shijie* (China Computerworld), 11 August 1997 No 30 p 21, as translated by FBIS 8/11/97.
[83] See Wang Xusheng, Su Jinhai and Zhang Hong, PLA Academy of Electronic Technology, *Jisuanji Shijie* (China Computerworld), 11 August 1997 No 30 p 21, as translated by FBIS 8/11/97

IW Institutions – Military

An article in the Spring of 1999 spoke of two books, one of which was reviewed in a 7 December edition of *Jiefangjun Bao.*[84] The article noted that these books formed the foundation for a cross-disciplinary course on IW at the PLA's Communication Command Academy.

> "The formal establishment of information warfare command and control within the Army. The Academy at present is deeply engaged in information warfare research. It has set up an information warfare curriculum on the PhD level, which is expanding the two volume's 22 chapters and branching into related areas. Five such sub-disciplines have been identified, including 'information warfare psychology' and 'information warfare transmission.'...The academy has already trained four groups of more than 300 experts in IW and has sent specialists to lecture at headquarters organizations, military units and service academies."[85]

An article in the 17 November 1999 edition of *Beijing Xinhua* noted one of the new institutes was tasked to assist with training talented individuals for the PLA's IW activities.

> "The newly established Information Engineering University attached to the PLA will cultivate professionals for future hi-tech warfare involving the use of information technology. Maj. Gen Zhou Rongting, president of the university made this remark recently in an exclusive interview with Xinhua. The new PLA University is located in Zhengzhou, the capital of Henan Province, was founded through the merger of three military schools in the same city, the Information Engineering Institute, the Measuring Institute and the Electronic Technology Institute."[86]

Perhaps most importantly, this article notes the establishment of "the National Defense Science, Technology and Information Center" in the PRC, which the authors claim will establish an IW simulation center. [87]

> "The Chinese military recently established a university of science and technology to train technological personnel for information

---

[84] See "PLA Trains Information Warfare Specialists" *Beijing Keji Ribao*, 27 April 99, as translated by FBIS 4/27/99

[85] See "PLA Trains Information Warfare Specialists" *Beijing Keji Ribao*, 27 April 99, as translated by FBIS 4/27/99

[86] See "University To Foster Talent for High-Tech Warfare" *Beijing Xinhua*, 17 November 1999. As translated by FBIS 11/17/99

[87] See "PRC. Taiwan Modern Warfare Viewed", *Chung-Yang Jih-Pao*, Internet Version, 11/22/99. As translated by FBIS 11/22/99.

warfare and to study information warfare theories and related technology. The People's Liberation Army [PLA] University of Science and Engineering was established after a merger of the Communication Engineering Institute, the Engineering College for Engineering Corps, the Air Force College of Meteorology, and 63 research institutes of the General Staff Headquarters. University President Major General Si Laiyi said that after a merger of colleges, the newly established 'Institute of Computer and Command Automation' set up six disciplines, including electronic engineering, information engineering, network engineering, command automation engineering, and counter-information, with key information warfare technology as the core.... There are over 400 experts and professors at the university conducting technological renovation. The university is planning to select 60 doctoral students every year to boost the ranks of instructors and set up five posts of special professors in major disciplines to attract outstanding young and middle-aged experts at home and from abroad."[88]

"Chinese experts in military affairs have proposed a concept along the following lines: That China establish an IW simulation training center, and that this center be staffed with experts dealing with every facet of IW, using the most advanced technical equipment and high-tech methods to create a simulated IW environment and carrying out training in simulated countermeasures. The center's staff will be composed of two types of personnel. First, will be the expert personnel. The main responsibilities that they will undertake include the tackling of key S&T problems, demonstration and proving of equipment, carrying on theoretical research and finally, teaching and guiding other staff members. The second type of personnel will consist of a small contingent of information technology specialists. This is a contingent specializing in the digitization of communications technology, integration of command, control, communications and intelligence functions, the fitting of weapons with smart features and the networking of the various types of warfighting systems. The main responsibilities to be undertaken by this contingent include testing, demonstrating and simulating various countermeasures." [89]

[88] See " PLA Trains Pesonnel for Information Warfare" *Tai Yang Pao*, Hong Kong 15 Sep 1999, as translated by FBIS 9/15/99

[89] See Weiguang Shen *Zhongguo Guofang Keji Xinxi* (China Defense Science and Technology Information), Sept-Dec 1996 No 5/6 p87-89. As translated by FBIS 9/1/96

As stated in the introduction of this paper, the Chinese recognize that IT will develop quickly in the civil sectors, but will have a latent symmetry to the military sectors as knowledge transfer travels from the former to the latter.[90] It is also these IT companies that will likely render substantial economic gains for the PRC economy. IT companies, specifically, telecommunications companies wanting to form subsidiaries in China, are one of the key features of WTO. For these reasons, it is important to establish institutions in both the civil and military sectors.

The "golden" series of projects appears episodically in Chinese open writings. They refer to a series of projects originating in 1997.

> "In a recent interview with Xinhua, MEI (Ministry of Electronics Industry) Minister Hu Qili said that related projects, dubbed 'golden projects', cover almost all major fields in the Chinese economy. According to Hu, the 'Golden Bridge' project has led to the establishment of a nationwide public economic information network linking 24 major Chinese cities. Trial operations of the 'Golden Card' project, an electronic currency system, are underway in 12 provinces with six provinces currently handling partial interbank financial transactions. Tax departments in 350 cities have introduced the 'Golden Tax' project this year...MEI has proceeded under the leadership of the State Council, China's highest administrative body and has tried hard to organize and coordinate the undertaking of key IT projects." [91]

As mentioned in the Information Security section of this paper, China is attempting to regulate the internet. One key institution in this process is the Internet Information Center.

> "China Internet Information Center (CNNIC). Its' duties include: provide domain registration for Internet users, provide IP address allocation, provide registration services for autonomous system; provide network technology information such as policies, rules, procedures for log in, and users training information and home page and data base information on the network. China began its Internet connection in 1994. In May of 1994, the domain name system began to operate in China. So far, the following four networks have been built: China Science and technology Network (CSTNET); China Public computer Interconnecting Network (CHINANET); China Education and Research Computer Network

[90] See graphic on page 3 of this paper.
[91] See "China Expands Construction of State Information Projects" *Beijing Xinhua*, 5 Sept 97, as translated by FBIS 9/5/97.

(CERNET); and the China Golden Bridge Information Network (CHINAGBN).[92]

IW MILITARY EXERCISES

In 1999, the Beijing Military Region (MR) conducted an MR wide computer simulation whereby the entire system came under IW attack. However, as was noted previously, this is not a sound approach to exercising the ability to continue to function in an IW environment specifically, because the participants in the exercise have foreknowledge of the attack. One of the most difficult things in IW is the ability to definitively know whether or not you've been attacked, or if you have enduring problems from some other, more benign source. Thus, these exercises, while indicative of an interest in CND, are not the best way to test such a case.

The first military exercise to focus on IW was held in March 1997 in the Shenyang MR, which is the MR north of the Korean Peninsula. It is noted for being the elite MR.

> "A few days ago, the Shenyang MR organized relevant units to hold an information warfare confrontational exercise in NE China involving content such as information interruption and counter-interruption, information deception and counter-deception, and information assaults and counter assaults. This advanced the units' information warfare research from theory to practical application by actual troops."[93]

The 1999 exercise in the Beijing MR was discussed in an 8 November 1999 article in *Jiefangjun Bao*.

> "One hundred generals and field officers were taking part in an exercise on the computer network. A 'war' without the smoke of gunpowder was quietly fought over an area of several hundred kilometers in North China a few days ago. For five days running two army groups under the Beijing Military Region, directed, dispatched by a direction, department of the leading organs, conducted a new sort of confrontation, campaign on the computer network...The exercise mainly practiced reconnaissance and counter-reconnaissance interference and counter-interference, blocking up and counter-blocking up an air strikes and counter-air strikes. The *direction department* set up from time to time, *unexpected situations* for both sides, compelling the commanders

[92] See Tao and Likun, "China Internet Information Center Established in Beijing" *Beijing Jisuanji Shijie* [Beijing Computer World], 9 June 1997 No 21, p1, as translated by FBIS 6/9/97

[93] Xu Sheng, Geo Jianlin, "Accept a New Challenge, Exercise in New Topics..." *Jiefangjun Bao*, 30 March 1998, as translated by FBIS 3/30/98

> of both blue and red armies to use their brains and display their courage... this was the first time the armed forces conducted on the computer network confrontation at the campaign level between a red army and a blue army."[94]

IW Case Study: PRC – Taiwan Crisis 1999

> "'The purpose of mainland China to increase military aircraft sorties in the Taiwan Strait area is to wage psychological warfare against Taiwan and to wreak havoc on the Taiwan stock market,' he said, adding that 'appropriate actions will be taken in case the activities of mainland Chinese war planes endanger the safety of civilian aircraft over the Taiwan Strait'... Gen. Tang urged the general public not to believe the rumors being spread by mainland China through Hong Kong news media. He refuted as 'totally untrue' a report on the Internet, which said a fierce air battle between the war planes of Taiwan and mainland China took place over the Taiwan Strait on Friday." [95]

Some of the more recent articles in the Asian open press relate to Chinese IW efforts against Taiwan. China and Taiwan entered into a third period of crisis[96], according to Chinese sources, in the summer of 1999 when Taiwanese President Lee Teng-hui announced his "state-to-state" policy. This comment re-opened the issue of Taiwan's reunification with the mainland and prompted a heated propaganda campaign that culminated in extensive military exercises in the Fujan province opposite the Taiwanese straits. Concurrent with these exercises were extensive discussions on China's ability to conduct IW against Taiwan. Hopefully, as the issue of Taiwan's reunification continues its discourse, Beijing will be mindful of one of Sun Tzu's teachings.

> "generally in war the best policy is to take a state intact; to ruin it is inferior to this."[97]

It would seem that Beijing has remembered this teaching, and is one of the primary reasons IW is so attractive to them in their arsenal against Taiwan. They

---

[94] Hong, Yang, "Beijing MR conducts Computer Exercise", *Jienfangjun Bao* (Internet Version), 8 Nov 1999. As translated by FBIS 11/8/99. It should be noted, when China uses the terms Red/Blue, they are Blue and the enemy is red; just as in the US. The "direction department" Refers to the control group, and the "unexpected situations" refers to what is known in the exercise jargon as "freeplay". Freeplay is a non-scripted segment of the exercise – most segments are highly scripted - such that the enemy has no foreordained knowledge of what might be presented to him. Freeplay exercises attempt to make the scenario more realistic by introducing uncertainty.

[95] See Taiwan Central News Agency, 07 Aug 99, as translated by FBIS 8/7/99

[96] The first was 1955, the second 1958

[97] Sun Tzu p77

believe that IW would limit collateral damage and not kill Taiwanese people, who after all, are Chinese.

In the Interview with a Taiwanese Air Force Officer, he states,

> "The CPC (China) started working on information warfare in 1985. Since 1995, it has been conducting various types of actual experiments. In 1997, it conducted a mock computer virus attack at the Nanjing Military Region, and in the same year, the Beijing Military Region conducted an experiment on attacking a broadcasting station with viruses. In summer 1999, the Lanzhou Military Region also conducted various exercises in information warfare. The National Defense Science and Technology Information Center[98] is the core component of information warfare development efforts. It has made significant achievements. Electromagnetic pulse weapons, such as neutron bombs, constitute a special threat."[99]

Another source, this one, from the Taiwan *Central News Agency*, on 10 November 1999, had the following to offer,

> "In a dispatch from Beijing, a correspondent from *The Australian* on Wednesday reported that China's new emphasis on cyberwar represents a policy U-turn, reversing decades of military planning because of its growing tensions with Taiwan and the West, particularly the United States. The daily reported that China's PLA recently completed its first full-scale simulation of a virtual war, involving hundreds of officers from artillery, airborne and armored divisions...Taiwan and Falun Gong sect have reported that Chinese computer hackers have attacked their information pages with pro-Beijing propaganda...The daily quoted Dick Clarke of Washington's National Security Council as saying that an electronic Pearl Harbor was a realistic prospect. 'We could wake up one morning and find a city, or the country, or a section of the country without power because of a surprise electronic warfare attack' he said."[100]

---

[98] For more on this Center, see Appendix B.

[99] Yajima, Seiji, "Taiwan Air Force Officer on Information Warfare with PRC", *Tokyo Sankei Shimbun* (Internet Version), 5 November 1999 as translated by FBIS 11/6/99. This author mistakingly refers to the '97 exercise as occurring Nanjing, it was Shenyang, and the December 1999 exercise was in Beijing MR.

[100] Chen, Peter "PRC said Preparing for Cyberwar with Taiwan and West", *Taiwan Central News Agency*, 10 November 1999, as translated by FBIS 11/10/99

The PRC propaganda campaign against Taiwan was openly admitted in a July 21, 1999 article in Hong Kong's *Tai Yang Pao*.[101]

Even the 1998 book "Unrestricted Warfare" speaks to the Taiwan situation.

> "The sensational book 'Transfinite Warfare[102] is actually a monograph that presents a scenario of future warfare. It makes it clear at the outset that "nonmilitary war behavior" is the primary concept of 'transfinite warfare.'... Upon mentioning the 1996 maneuver and a number of maneuvers that the mainland has conducted in the recent past, Wang Xiangsui [one of the authors of the book] maintained that these are real examples of the mainland applying "transfinite warfare" without realizing it, in the campaign to prevent Taiwan independence. What the mainland is conducting now is a combination of diplomatic warfare, economic warfare, media warfare, and deterrence warfare, with a view to bringing about a political solution.... The 1996 maneuver in the Taiwan Straits sent a message to the international community, that the mainland does take the Taiwan issue absolutely seriously and that there is no leeway. This is a line that everybody must abide by according to the international rules of game. This played a very important role in influencing the international community's attitude toward Taiwan and also acted as a deterrent as far as the Taiwan authorities were concerned... But why is such an option not taken? Military strikes would be easily effected, sending hundreds of thousands of troops across. But what happens then? Should we keep a watch on the tens of millions of people in Taiwan? Should we set up a provincial CPC committee and a provincial government? It is therefore clear that the military approach is not a conclusive solution to the problem. A political solution is still needed and we should wait for the time when the conditions are ripe... He maintained that some of the mainland's recent maneuvers [i.e., 1999] were not necessarily directed at Taiwan. The purpose of maneuvers is to test specific data of experimentation, rather than to bluff and bluster."[103]

> "Of the attacks of this nature that Beijing might launch against Taiwan, Lin warned the general public to pay special attention to the so-called EMP (electronic magnetic pulse) tactic." [104]

---

[101] See Kuo-Chung, Tsao, "Mainland's Propaganda Offensive Enters Second Stage", *Tai Yang Pao*, Hong Kong, 21 July 1999. As translated by FBIS 7/21/99

[102] This is another translation of the term "Unrestricted," thus, this article refers to the book "Unrestricted Warfare" by Wang Xiangsui and Qiao Liang.

[103] See "Ingenious Remarks by Author of 'Transfinite Warfare' on Using Force Against Taiwan", *Tai Yang Pao*, Hong Kong 24 November 1999, as translated by FBIS 11/24/99

[104] See Lee, Bear "Expert Warns Against PRC's Information Warfare" *Taiwan Central News Agency* 31 May 1999, as translated by FBIS 5/31/99

Taiwanese Response

Taiwan is not sitting back and taking the exercises across the straits casually. One Hong Kong text on 9 January 2000, noted Taiwan is developing its own computer attacks schemes.

> "The Taiwanese military has developed some 1,000 computer viruses that could be used to fight back in any Chinese invasion of the island, a report said Sunday...Several wargames held in China's Nanjing, Beijing and Lanzhou military districts since 1985 have focused on using electronic equipment to destroy enemy computer and communications systems, the defense ministry has said."[105]

In November of 1999, the Democratic Progressive Party (DPP) issued a Defense White Paper in which, IW was the first measure of defense mentioned in Chapter Three entitled "Military Strategies", and was cited as the 'trump card' for defense of Taiwan.

> "The national army should seize the key of the modern warfare by giving priority to developing information warfare capability an the research, manufacturing, and deployment of long-range, precision guided weapons and use our information superiority, command of the air space over the Taiwan Strait...we can use that [long range precision guided strike capability] in conjunction with our effective forestalling measures to seize immediate information superiority and air and sea command in the Taiwan Strait to inhibit or destroy the enemy's command and information system and sea and air combat and logistic supply capabilities... Therefore, the best choice for Taiwan's defensive operation at wartime is to suppress and interfere with the enemy's command and intelligence system, destroy and beat back the invading enemy planes and warships, paralyze the enemy's sea and air bases, strive to seize electromagnetic control and air command in the Taiwan Strait... *Information warfare will be the trump card in the Taiwan Strait defense operation in the future.* With respect to electronic information which plays a decisive and subversive role in the modern warfare, the national army should upgrade its composite C4ISR system its 'multiple combat capabilities.' At the same time, we should purchase planes and equipment for electronic warfare and actively engage in the research and development of codes for electronic information warfare to strengthen our ability to suppress the enemy and use our information superiority to effectively control

[105] See Hong Kong AFP, 9 January 00; as translated by FBIS 9 January 2000.

the scale of confrontation in the Taiwan Strait... In addition, because of its characteristics, the ramifications of a modern war will be much broader, and therefore when war breaks out, public and private sectors that include the government and civilians will be affected. In particular, in the information warfare era, the relationship between civilian forces and the war itself will be much closer than ever before." [106]

Conclusions:

The IT revolution is offering the military commander unimagined possibilities for collecting, processing, and analyzing data so critical to transparent battlefield operations. This revolution is producing improvements in computer capabilities in orders of magnitude, and the civilian sectors, both in the US and in China, are leading these efforts. Absolutely critical to this process is having accurate information. As Marxist/Maoist students would note, the dialectic of the IT phenomenon suggests that if this critical information can be compromised somehow, this one act will render a disproportionate impact throughout the military campaign. Thus, information warfare is taking a central place in current and future military operations.

The US and China view IW very differently. These differences stem from not only their different current force structures, but also different military history and experiences. The Chinese have argued that the father of IW was the military theorist Sun Tzu, who wrote in 500BC. There is some truth in this statement – Sun Tzu did write about concepts, such as PSYOPS, D&D, that are now central to IW. But Sun Tzu could not imagine what computing capability would do to information management and manipulation. Differences also stem from the US seeing IW as one part of their military capability, whereas in China, the perception management function of IW is a way of life in both their military and civilian sectors.

There is ample evidence to suggest that China is developing active integration of IW into their military doctrine and strategy, and that this integration will follow both a symmetric and an asymmetric path. It is obvious from examining these efforts in the context of the six pillars of IW that China is further along in some pillars than in others. It is equally obvious that they intend to include in IW concepts such as above-war methods and non-applicable war methods, and that they have already begun to do so, using Taiwan as test case. These tenets of IW have no parallel in US IW efforts. China lags behind the US in some aspects, particularly CND, but is undertaking efforts to correct these shortfalls, to include IW in their military exercises. They have also expended much effort and funds to acquire some of the latest C4ISR systems that will greatly improve their reconnaissance and surveillance capabilities, on which a successful military

[106] See "Taiwan's DPP Issues Defense White Paper", 23 November 1999, as translated by FBIS 11/23/99

campaign, and IW depend. They are also in the process of establishing and empowering institutions, both in the military and civilian sectors, to ensure consistent and continued attention to IW issues.

Lastly, the Chinese recognize that they must rise to the IT challenge, in the military sector in particular.

> …the turn of the century presents a grim challenge to our army…our country has a poor and meager foundation and we are lagging a long way behind developed countries in high technologies – especially in information technologies. If we take the matter lightly and let the opportunity slip past, we will once again be discarded by history when developed countries have completed their work on building an information army by the mid 21st century –
>
> Wang Baocun , Sr. Col.

BIBLIOGRAPHY

Binnendijk, Hans and Montaperto, Ronald, "Strategic Trends in China", National Defense University, 1998. See www.ndu.edu/inss/books/china/chinacont.html.

Fast, William R., LtCol, "Sun Tzu Art of War in Information Operations", National Defense University, Washington DC, 1998. www.ndu.edu/ndu/inss/siws/ch.1 .html

Garver, John W., *Face Off: China, the United States and Taiwan's Democratization*, University of Washington Press, 1997

Glaser, Bonnie, "US-China Challenged by New Crises", *Comparative Connections*, Quarterly E-Journal on E. Asian Bilateral Relations, edited by Ralph A Cossa and Rebecca Goodgame Ebinger, Vol I, Issue I, July 1999 – 2nd Quarter.

Griffith, Samuel, "*Sun Tsu, The Art of War*", Oxford University Press, 1963

Harding, Harry, *China's Second Revolution: Reform after Mao"*, Brookings Institute, Washington DC 1987

Hull, Andrew, "The *Chinese Approach to Information Warfare*", Institute for Defense Analysis, 1998 (unpublished paper)

Joint Pub 3-13, "*Joint Doctrine for Information Operations*", Publication of the Joint Staff, 9 October 1998

Levien, Fred "Information Warfare: The Plain Truth" *Janes Defense Weekly*, April 1999. www.jedefense.com/jed/html/new/apr99/technology.html

Lilley, James R and Shambaugh, David et al, "*China's Military Faces the Future*", ME Sharpe 1999. This reference is a collection of articles by various authors – Tai Ming Cheung; June Teufel Dryer; Richard D. Fisher, Jr; Wendy Frieman; Bates Gill; Paul Godwin; Taeho Kim; Eric McVadon; and Michael Pillsbury.

Pillsbury, Michael, "*Chinese Views of Future Warfare*", National Defense University, Washington DC, 1998

Segal, Gerald, "Take Off the Rose-Colored Glasses: It's the Same China", *PACNET NEWSLETTER*, 1/99, Center for Strategic and International Studies, Johns Hopkins University, Washington DC. www.csis.org/pacfor/pac0499.html

Shambaugh, David and Richard Yang, *China's Military in Transition*, Clarendon Press, Oxford, 1997

Stokes, Mark A. "China's Strategic Modernization: Implications for the United States", US Army War College, Strategic Studies Institute, Carlisle PA, September 1999.

Storey, Ian James "Living with the Colussus: How SE Asian Countries Cope with China", *Parameters*, Winter 1999-2000 p 1111-125, US Army War College, Carlisle PA

STRATFOR.COM, "Year of the Crackdown", www.stratfor.com/asia/countries/china/chinapackage/uneasycrackdown1.html

See Tyler, Patrick *A Great Wall: Six Presidents and China*, Century Foundation, New York, New York1999

Waltz, Edward "The US Transition to Information Warfare" *Janes Defense Weekly*, December 1998

Witherspoon, Richard, COL, "Traditional Military Thinking and the Defensive Strategy of China: An Address by Lt.Gen Li Jijun, Vice President, Academy of Military Science of PLA" US Army War College, Strategic Studies Institute, Carlisle PA, August 1997.

Wik, Manuel W. "Global Information Infrastructure: Threats" www.globalcomms.co.uk/interactive/technology/280.html

Wortzel, Larry M. "China's Military Potential" Strategic Studies Institute, US Army War College, Carlisle PA, October 2, 1998. See Carlisle-www.army.mil/ usassi/ssipubs/pubs98/chinamil/chinamil.html.

APPENDIX A
Domestic and International Setting

China's Information Warfare (the wartime component of Information Operations), is part and parcel of their overall military buildup that has been ongoing since the 1980s, when their economic gains were truly noteworthy and caught the attention of the world. As a background to examining China's IW interest, one must understand the shifting strategic context of China in the late 1980s/early 1990s. Externally, China was shocked by the fall of the Soviet Union in 1990, the swift and overwhelming military capabilities demonstrated by the US Coalition forces during Desert Shield/Desert Storm, taken aback by the renewed US-Japanese treaties in 1996[107], and especially the TBMD program activities in the 1990s. Lastly, and perhaps most importantly, they felt a challenge to their entire legitimacy as a nation-state by the democratic processes in Taiwan of the early 1990s. Since 1949, they have said Taiwan is part of the PRC, as part of their "One China Policy." As expected, China watched very closely the US response to all of these matters. The Tienanmen massacre of 1989 colored Western perceptions of China throughout the early 1990s and some could argue even into the late 1990s.

Internally, Chinese politics were still in the consolidation phase under Jiang Zemin. Some analysts argued that because of this political balancing act, the People's Liberation Army (PLA), was achieving more influence over the political regime than had existed under Deng, who derived his legitimacy from his revolutionary heritage.[108] Economically, the strong showing of the Chinese economy of the 1980s, was hit in early 1990's by the Asian financial Crisis[109], but by late 1990s, seemed to have weathered the storm, although foreign investment had dropped dramatically, owing more to unsuccessful policies regulating foreign investment rather than the crisis itself.

As One American Sinologist put it,

> "On the other hand, modernization means that Peking will have greater material resources with which to pursue goals in international affairs and increasing Chinese nationalism raises the possibility that those goals may be defined in ways that compete or conflict with the interest of other Asian states." [110]

To this statement one could add "with the interest of other Asian states" *and the United States.*

---

[107] See Jordan, Mary, "Japan Approves Expanded Military Alliance with US", *Washington Post* May 25, 1999 p10

[108] See Garver, John W. *Face Off: China, the United States and Taiwan's Democratization,* University of Washington Press, 1997, page 43

[109] For an extensive overview on a country by country basis of this crisis, see "The Tigers that Changed their Stripes", *The Economist,* 2/12/00

[110] See Harry Harding, "*China's Second Revolution*" Brookings Institute, Washington DC 1987, p 246

This reference notes a very balanced assessment of the future possibilities based on China's success in its reform programs. There are indications both pro and con, that China will use their newfound wealth and prominence on the international stage to attempt to flex their muscle in their region – specifically, the Spratly Isls and Taiwan. Some analysts even point to an interest among some PLA –N (Navy) officers to build/acquire a truly blue-water sea-faring Navy spearheaded by a new CV, suggesting more than a regional influence. On the other hand, there is no mistaking the moderation of Chinese ideological stances – both in terms of supporting revolutionary regimes abroad, as Mao dictated; and in increasing freedoms (speech, travel abroad), personal economic choices, rising standards of living etc., of daily life within China. Regardless of the path China will follow, most people would agree it is a far better road than the one they have traveled to arrive at this point.

As an introduction, a similar point should be made that just because China seems to be interested in how information warfare should be adapted and applied to a unique Chinese style of warfare does not necessarily mean they have already done so, although there is evidence that they have. It remains to be seen whether they will be successful in doing so in the future – particularly the near term. As we will see, China's concept of IW is already distinctly Chinese in its orientation – being based far more on the eminent Chinese military theoretician Sun Tsu than accepting, in its entirety, US definitions of the concept. A discussion of topics does not necessarily imply intent. It can often be a venue for discussion and debate on matters prior to a major decision to move forward or discontinue efforts. As such, the US military analyst must undertake a more thorough evaluation of these discussions to investigate the next logical conclusion. For example, if discussion on computer network defense (CND) is prominent among Chinese writings, is there any evidence to suggest that they are purchasing on the world market, or having their own computer programmers write sophisticated encryption codes that would enable such discussions to become reality? If the answer is yes, then the "next step" would be to assess how well they have incorporated said technology. There is evidence in the unclassified literature for example, that China has held several military exercises under "computer attack" conditions, testing CND.[111]

[111] See for example, Hong, Yang, "Beijing MR conducts Computer Exercise", *Jienfangjun Bao* (Internet Version), 8 Nov 1999. As translated by FBIS 11/8/99

APPENDIX B
CHINESE INSTITUTES/ORGANIZATIONS INVOLVED IN IW

1. Chinese Electronics Society Beijing Yuguangtong S&T Development Center. REF: Li Nengjing, Beijing *Zhongguo Dianzi Bao* [China Electronics News], 24 Oct 1997 p 8, as translated by FBIS 12/29/97

2. PLA Academy of Electronic Technology REF: Wang Xusheng, Su Jinhai and Zhang Hong, Beijing *Jisuanji Shiji*, 11 August 1997 as translated by FBIS 8/11/97.

3. Department of Computer Science, *Journal of University of Electronic Science and Technology of China* REF: Liu Naiqi, Zuo Zhihong, *Journal of University of Electronic Science and Technology of China (UESTC)*, June 1997, Vol. 26 No 3 p 283-288 as translated by FBIS 6/1/97.

4. State Information Security Appraisal and Identification Management Committee. Responsible for protecting government and commercial confidential fields on the Internet, identifying any net user, and defining rights and responsibilities. REF: "Information Security Oversight Committee Formed"*Beijing Xinhua* 2/12/99, as translated by FBIS 2/12/99

5. Information Engineering University of the PLA. Responsible for providing high-quality military professionals in a variety of fields for modernization of national defense. REF: "PLA Information Engineering University set up" *Beijing Xinhua*, 2 July 1999, as translated by FBIS 7/2/99

6. State Science and Technology Commission, Chinese Academy of Sciences, and the State Commission of Science, Technology and Industry for National Defense. Publishes *Beijin Keji Ribao*, Daily newspaper of domestic and foreign science and technology. Article on 4/27/99 noted training of "digitized units" based on books cited in reference 1 below.

7. MEI (Ministry of Electronics Industry) Minister Hu Qili . MEI has proceeded under the leadership of the State Council, China's highest administrative body and has tried hard to organize and coordinate the undertaking of key IT projects." REF: "China Expands Construction of State Information Projects" *Beijing Xinhua*, 5 Sept 97, as translated by FBIS 9/5/97

8. China Internet Information Center (CNNIC). Duties include: provide domain registration for Internet users, provide IP address allocation, provide registration services for autonomous system; provide network technology information such as policies, rules, procedures for log in, and users training information and home page and data base information on the network. REF Tao and Likun, "China Internet Inforamtion Center Established in Beijing" *Beijing Jisuanji Shijie* [Beijing Computer World], 9 June 1997 No 21, p1, as translated by FBIS 6/9/97.

9. China Information Seciurity Evaluation and Certification Center, est. 4/99. Duties include standardizing the information security and service. REF: China Sets Up Information Security Evaluation Center, *Zhongguo Tongxun She,* Hong Kong 9 Apr 99, as translated by FBIS 4/9/99.

10. National Defense Science and Technology Information Network (NDSTIN). REF: Binghua, Liu, "Technical Attacks on Network Information Systems, Security Countermeasures" *Beijing Zhongguo Guofgang Keji Xinxi* (Chinese Defense Science and Technology Information, Jun 1997, as translated by FBIS 6/1/97

11. *Beijing Zhongguo Junshi Kexue* (China Military Science) JOURNAL

12. 8th Design Department of the 8th Academy of China's Aerospace Corporation. Duties: jamming. REF: Shjuigen, Zhou "Expert System for Enemy's Operational Intention Decision Based on Battlefield Electronic Jamming Information" *Shanghai Hangtian* (Aerospace Shanghai), October 1996 as translated by FBIS 10/1/96

13. China Information Center for Defense Science, Technology – "The Information Center has scored abundant results and brought up scientists and technicians one batch after another. It has a large number of scientists and technicians rich in experiences, who are well known inside and outside the Army, and has shaped a qualified people group, characterized by three-in-one combination of the old, middle aged and the young... REF: Xiangbing, Zhang "Information Center for Defense Science Viewed" *Jiefangjun Bao* 6 July 1997 as translated by FBIS 7/6/97

CHINESE SYMPOSIA/MEETINGS INVOLVED IN IW

1. Defense Information Modernization Symposium, held 15 Sept 1997, at PLA General Staff's Research Institute. REF: Li Nengjing, Beijing *Zhongguo Dianzi Bao* [China Electronics News], 24 Oct 1997 p 8, as translated by FBIS 12/29/97

2. Junshi Xueshu Magazine holds Symposium, as mentioned in *Jiefangjun Bao* 11/24/98.

3. All China Computer Security Conference 1993. REF: Naiqi, Liu et al "Computer Virus Countermeasures, Virus Warfare" *Chengdu Dianzi Keji Daxue Xuebao* [Journal of Unviersity of Electronic Science and Technology of China), June 1997, Vol 26, No3 p 283-288 as translated by FBIS 6/1/97

3. Fire Control and Command/Control Conference, sponsored by the journal *Huoli Yu Zhihui Kongzhi*, October 1996 as translated in FBIS 10/1/96

4. 15 Sept 1997 Defense Information Modernization Symposium organized by the Chinese Electronics Society, Beijing, Yuguangton S&T Development Center and Zhongguo Dianzi Bao (China Electronic News), held at PLA General Staff's Research Institute REF: *Zhongguo Dianzi Bao* 10/24/97 as translated by FBIS 10/14/97

BOOKS

1. "Command and Control in Information Warfare" and "Technology in Information Warfare" edited by Si Laiyi, Commandant of the Communications Command Academy, were recently published by the Liberation Army Publishing House. REF: Yuanshen, Lei, "New Breakthrough in Study of Information Warfare", *Jiefangjun Bao* 21 Jul 1998, as translated by FBIS 7/21/98