Issues & Studies© 39, no. 2 (June 2003): 107-143.

China's Information Warfare Discourse: Implications for Asymmetric Conflict in the Taiwan Strait*

VINCENT WEI-CHENG WANG

This paper discusses the emerging discourse on, and capability of the PRC in, information warfare (IW)—as well as the implications of such developments for cross-Strait and U.S.-PRC relations. Chinese discourse shows that informed PLA officers realize that IW constitutes the war of the future and plays a critical role in the Revolution in Military Affairs (RMA) —a key step necessary for China's military modernization. One allure of this type of warfare is the potential for China to wage an "asymmetric war" —i.e., the use of surprise force by a weaker party against a stronger but vulnerable adversary—by applying traditional stratagems. The Chinese argue that using such traditional maxims as Sun Tzu's "overcoming the superior with the inferior" and Mao Zedong's "people's war" in modern war-

---

VINCENT WEI-CHENG WANG (王維正) is Associate Professor of Political Science, University of Richmond, Virginia, USA. In Spring 2003, he is Visiting Associate Professor of Political Science at the National Sun Yat-sen University, Taiwan. The author would like to thank the two anonymous reviewers of *Issues & Studies* for their suggestions, Gwendolyn Stamper for contributing to early stages of this project, Gregory Surber for his research assistance, the University of Richmond for a faculty-student collaborative research grant, and the *American Asian Review* for permission to use portions of a different paper published in *AAR*'s December 2002 issue; he dedicates this article to his father, the late Mr. Ming-kao Wang. Dr. Wang can be reached at <vwang@richmond.edu>.

*An earlier version of this paper was presented at the annual meeting of the American Political Science Association's Conference Group on Taiwan Studies (CGOTS), Boston, August 31-September 3, 2002.

fare would both counter overall American strengths by focusing on certain "pockets of excellence" and present China with a credible military option for achieving its political objective of unification with Taiwan (on Beijing's terms). These strategic considerations could, however, introduce instability into the Taiwan Strait; they also challenge conventional wisdom in international relations. This paper critically evaluates the doctrinal-capability gap in China's IW development—the double-edged nature of technology, the low connectivity of Chinese society, and Taiwan's responses—and concludes with a cautionary note on an emergent digital "mutual assured destruction" (MAD) dynamic across the Taiwan Strait.

KEYWORDS: **information warfare; asymmetric war; unrestricted warfare; cross-Strait relations; Sun Tzu.**

* * *

"War is a matter of vital importance to the State; the province of life or death; the road to survival or ruin. It is mandatory that it be thoroughly studied."

—Sun Tzu (孫子)[1]

In September 2002, Taiwan President Chen Shui-bian (陳水扁) warned that the People's Republic of China (PRC) had been developing strategies to wage unrestricted warfare (超限戰, *chaoxian zhan*) against Taiwan. Chen explained that, in contrast to traditional warfare, unrestricted warfare would include using such tactics as the fifth column, cruise missiles, electromagnetic pulse attacks, biochemical weapons, and computer network hacking to launch a surprise attack against Taiwan's infrastructure, command and control system, and political, economic, and financial centers.[2] Chen's speech, delivered on the eve of the first anniversary of the September 11 terrorist attacks on New York City and Washington, D.C., underscored Taiwan's anxiety over the increasing threat posed by the rapid modernization of both the capabilities and doctrines of the People's Liberation Army (PLA).

---

[1]Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (Oxford: Oxford University Press, 1963), opening statement.

[2]"Dalu junshi weihe bi kongbu geng lihai" (Mainland China's military intimidation is more serious than terror), *BBC Chinese.com*, September 10, 2002, available online at <http://news.bbc.co.uk/hi/chinese/news/newsid_2248000/22482941.stm>.

Viewed from a politico-military standpoint, the heightened attention paid to unconventional forms of warfare signifies that the complex cross-Strait relationship is entering a new—and arguably—unstable, era. Up until the present, despite having witnessed spasmodic flareups, the cross-Strait relationship is essentially a political stalemate with no imminent military crisis on the horizon. To a large extent, two layers of deterrence—resistance by Taiwan's armed forces and the possible but not preordained intervention by the United States—have thwarted any PLA military adventure against Taiwan.

The hitherto absence of war in the Taiwan Strait can be "explained" by two aphorisms that have been widely (and perhaps also uncritically) accepted by most international relations scholars and security analysts: (1) in a conflict, the party with preponderant force prevails—either by coercing the weaker party to take an action desired by the former (i.e., a situation of compellence) or by dissuading the weaker party from taking an action detested by the former (i.e., deterrence); and (2) despite refusing to renounce the use of force against Taiwan, the PRC currently possesses few credible military options. As this paper will demonstrate, however, certain recent developmental trends in the PLA could upset the status quo in the Taiwan Strait.

In recent years some well-versed military theorists and writers in the PLA have been exploring new concepts of war that call into question, if not invalidate, these two dictums. Of particular note is the PLA's fascination with asymmetric warfare strategies that make offense a more attractive option to the weaker party.[3] One publication that has attracted considerable attention inside and outside China is *Unrestricted Warfare*.[4] The authors,

---

[3]For more discussion on the concept of "asymmetric conflicts," see Thazha V. Paul, *Asymmetric Conflicts: War Initiation by Weaker Powers* (New York: Cambridge University Press, 1994); Ben D. Mor, "'Asymmetric Conflicts': War Initiation by Weaker Powers," *American Political Science Review* 90, no. 1 (March 1996): 234-36; and Ivan Arreguin-Toft, "How the Weak Win Wars: A Theory of Asymmetric Conflict," *International Security* 26, no. 1 (Summer 2001): 93-128.

[4]Qiao Liang and Wang Xiangsui, *Chaoxian zhan* (Unrestricted warfare) (Beijing: Jiefangjun wenyi chubanshe, 1999), available online at <http://www.shuku.net:8080/novels/wars/cxzh/cxzh.html>. An English translation, provided by the CIA's Foreign Broadcast Information Service (FBIS), can be found at <http://cryptome.org/cuw01.htm>.

who are both PLA colonels, envision the future of warfare as the following:

> War in the age of technological integration and globalization has eliminated the right of weapons to label war... while the appearance of ... new concepts of weapons has gradually blurred the face of war. Does a single "hacker" attack count as a hostile act or not? Can using financial instruments to destroy a country's economy be seen as a battle? Did CNN's broadcast of an exposed corpse of a U.S. soldier in the streets of Mogadishu shake the determination of the Americans to act as the world's policeman, thereby altering the world's strategic situation? And should an assessment of wartime actions look at the means or the results? Obviously, proceeding with the traditional definition of war,... there is no longer any way to answer the above questions. When we suddenly realize that all these non-war actions may be the new factors constituting future warfare, we have to come up with a new name for this new form of war: warfare which transcends all boundaries and limits, in short: unrestricted warfare.

They continue on to identify the characteristics of unrestricted warfare:

> [T]his kind of war means that all means will be in readiness, that information will be omnipresent, and the battlefield will be everywhere. It means that all weapons and technology can be superimposed at will, it means that all the boundaries lying between the two worlds of war and non-war, of military and non-military, will be totally destroyed, and it also means that many of the current principles of combat will be modified, and even that the rules of war may need to be rewritten.[5]

This paper discusses the emerging discourse on, and capability of the PRC in, information warfare (IW)—as well as the implications of such developments for conflict in the Taiwan Strait. Three reasons justify a focus on IW. First, IW exemplifies unrestricted warfare and lends credence to the concept of asymmetric war. It challenges the conventional Clausewitzian view that "violence is the essence of war" by luring the initiators of IW into thinking that they can achieve their political objectives without much sacrifice. Note that the Chinese view IW as a superior choice for attaining classic strategist Sun Tzu's adage: "To subdue the enemy without fighting is the acme of skill."[6]

Second, many nations rely on information systems in the operation of their militaries, economies, and governments. This dependence on in-

[5]These two quotes are from FBIS translation, ibid.

[6]Sun Tzu, *The Art of War*, 77.

formation technology (IT) will only further increase under globalization, rendering the distance factor (geographic contiguity or force projection) irrelevant in war calculus. "Information systems now serve as both weapons and targets of warfare," declares Greg Rattray, the former commander of the U.S. Air Force Information Warfare Squadron.[7] With dedicated responsibilities for defending the United States from IW, Rattray worries that "the growing reliance of U.S. society on information infrastructures creates potential new centers of gravity for enemy attack in strategic warfare based on disrupting and defending these infrastructures."[8]

Third, certain trends in the cross-Strait IT trade—such as the growing number and sophistication of Taiwan IT firms investing in the PRC as well as China's emergence as the world's fastest-growing (and one of the largest) IT producers—portend far-reaching changes in the cross-Strait balance of power.[9] Fundamentally, developing IT constitutes a critical strategy in China's quest for greater international power.[10] History is replete with cases wherein technology alters the nature of war. Although a full discussion of this point is beyond the scope of this paper, the general gist of this argument should suffice to highlight the importance of the current study.

This paper's main arguments are highlighted at the outset. First, the

---

[7]Greg Rattray, *Strategic Warfare in Cyberspace* (Cambridge, Mass.: MIT Press, 2001), 8.

[8]Ibid., 101.

[9]For a study on the impact of China's rising IT industry on Taiwan's economy, see Peggy Pei-chen Chang and Tun-jen Cheng, "The Rise of the Information Technology Industry in China: A Formidable Challenge to Taiwan's Economy," *American Asian Review* 20, no. 3 (Fall 2002): 125-74. For a work that expounds on the "Silicon Valley-Taiwan-Shanghai IT corridor" thesis, see Tse-Kang Leng, *Zixun chanye quanqiuhua de zhengzhi fenxi: Yi Shanghaishi fazhan weili* (A political analysis of the globalization of information industries: A case study of Shanghai) (Taipei: Ink, 2002).

[10]For a new book that examines the IT rivalry for increased international power between China and India, the world's two most populous nations, see Marcus Franda, *China and India Online* (Lanham, Md.: Rowman & Littlefield, 2002). On the integration of the economies of Taiwan and the mainland as spearheaded by the electronics industry, see Barry Naughton, ed., *The China Circle: Economics and Technology in the PRC, Taiwan, and Hong Kong* (Washington, D.C.: Brookings Institution, 1997). On China's attempt to leap into the "information age" while retaining its unique socialist market characteristics, see Milton Mueller and Zixiang Tan, *China in the Information Age: Telecommunications and the Dilemmas of Reform* (Westport, Conn.: Praeger, 1997, for the Center for Strategic and International Studies, Washington, D.C.).

PRC's interests in IW reflect an increasingly prevalent view among strategic thinkers in China that IW is a key catalyst for the PLA's Revolution in Military Affairs (RMA) and a vital impetus for its military modernization.

Second, China's IW strategy is distinctive in applying traditional stratagems (e.g., Sun Tzu's "overcoming the superior with the inferior" and Mao Zedong's [毛澤東] "people's war") to modern warfare in an attempt to overcome a technologically superior adversary (i.e., the United States) by attacking its strategic "Achilles' heel." China's IW strategy thus epitomizes asymmetric war.[11]

Finally, China is determined to seek to develop its IW capability into a credible military option: (1) for the absorption of Taiwan on Beijing's terms at some point in the future, and (2) in order to deter the United States from intervening in any cross-Strait conflict.[12] These trends increase the prospects for misperception and miscalculation and introduce new sources of instability into the cross-Strait relationship.

For these reasons, a study of China's IW strategies is both timely and important. This paper will examine China's IW discourse and capability by focusing on the political objectives of China's IW and the implications of asymmetric warfare.

The New War

Scholars have long been grappling with the impact of information

[11]This is corroborated in the July 2002 Pentagon report to the U.S. Congress, which states that China "views information operations/information warfare (IO/IW) as a strategic weapon..." and "is particularly sensitive to the potential asymmetric applications IO/IW can have in any future conflict with a technologically superior adversary." See Department of Defense, "Annual Report on the Military Power of the People's Republic of China" (Report to Congress pursuant to the FY2000 National Defense Authorization Act, July 12, 2002), available online at <http://www.defenselink.mil/news/Jul2002/d20020712china.pdf>.

[12]A Pentagon report points out that China's military is developing strategies and tactics to use "surprise, deception, and shock" in any opening military campaign, while "exploring coercive strategies" designed to bring Taiwan to terms quickly. See Department of State, "China is Considering a Coercive Strategy on Taiwan, DOD Says," e-mail update sent by Office of International Information Programs, U.S. Department of State <uschinapd@YAHOO.COM> to <US-CHINA@LIST.STATE.GOV> (July 16, 2002).

technology on international relations.[13] Experts have especially warned that the information revolution is enabling both new forms of organization and new doctrines that will affect the spectrum of conflict, including terrorism.[14]

In the aftermath of September 11, the prospect of "cyberterrorism" presents an especially frightening scenario to the world's only superpower —the United States. These terrorist attacks were characterized by their asymmetric war nature: a weaker party utilizing surprise, deception, and shock against a stronger party.

Some scholars call September 11 "globalization's first war," arguing that what the terrorists attacked was globalization itself.[15] Most also believe, however, that globalization will bounce back. Globalization will continue to help facilitate the diffusion of information technology, which many view as globalization's quintessential hallmark.[16] This seemingly unstoppable trend may enable various state and nonstate actors (many with grievances toward U.S. power or policy) to eventually attain the technological skill or opportunities to wreck havoc against the United States.

Chances for such IW are not so remote. In the United States, the computer network is controlled by the private sector (i.e., those numerous companies whose main motive is profit), whereas defending national security falls under the purview of the military.[17] America's very strength, i.e., openness and accessibility of information, could turn into its Achilles' heel—if an adversary can exploit this weakness.

---

[13]See Robert O. Keohane and Joseph S. Nye, "Power and Interdependence in the Information Age," *Foreign Affairs* 77, no. 5 (September/October 1998): 81-94.

[14]John Arquilla, David Ronfeldt, and Michele Zanini, "Information-Age Terrorism," *Current History* 99, no. 4 (April 2000): 179-85.

[15]Kurt M. Campbell, "Globalization's First War?" *The Washington Quarterly* 25, no. 1 (Winter 2002): 7-14; and Strobe Talbott and Nayan Chanda, eds., *The Age of Terror: America and the World After September 11* (New York: Basic Books for the Yale Center for the Study of Globalization, 2002), vii-viii.

[16]See Thomas L. Friedman, *The Lexus and the Olive Tree* (New York: Farar, Straus, & Giroux, 1999), 39-58.

[17]John Galvin, "Info War: The Enemy's Camp is a Cube on the Other Side of the Globe. Their Targets? Your Business," *Ziff Davis Smart Business for the New Economy*, June 1, 2001, 72.

In 1999, John Hamre, U.S. Deputy Secretary of Defense, warned about the possibility of an "electronic Pearl Harbor" launched by hackers against American commercial interests.[18] James Adams, an Internet security expert, has gone as far as to say that the virtual world is where the next war will be waged because, for the first time in history, the weapons are available to everyone.[19]

These trends are of keen interests to many of America's detractors. Dan Kuehl, a professor at the U.S. National Defense University, lists China, Russia, Iraq, Libya, terrorist groups like Al-Qaeda, and even unsavory organizations in friendly nations as "cyberthreats."[20] In 1998 CIA Director George Tenet warned the Senate Government Affairs Committee that intrusion into government computers would become increasingly more sophisticated and better organized, with potential attackers including "national intelligence and military organizations, terrorists, criminals, industrial competitors, hackers, and disgruntled or disloyal insiders." While declining to name names, Tenet confirmed that several nations had been working on developing an information warfare capability.[21]

Just what is information warfare and how is it implemented? According to John Alger, former dean of the National Defense University's School of Information Warfare and Strategy, IW "consists of those actions intended to protect, exploit, corrupt, deny, or destroy information or information resources in order to achieve a significant advantage, objective, or

---

[18]"Pentagon Officials Warn of an Electronic Pearl Harbor," Associated Press, March 9, 1999 (accessed via *Lexis-Nexus*).

[19]James Adams, *The Next World War* (New York: Simon & Schuster, 1998), gives an exhaustive history of information warfare, as well as U.S. military capabilities in this area. He states categorically that the Air Force can track hackers back to their computers and strike back with "computer bombs." However, many of America's enemies also have the same skills.

[20]Cited in Galvin, "Info War" (see note 17 above).

[21]While Tenet declined to name those countries, Committee Chairman Fred Thompson (R-Tenn) was not as reticent. Citing reports, Thompson named China, Russia, Libya, Iraq, Iran, and at least seven other countries as developing IW programs. See "CIA Director Warns of Intrusion into Government Computers," Associated Press, June 24, 1998 (accessed via *Lexis-Nexus*); and Jennifer Mateyaschuk, "Nothing to Raise a Glass About," *Information Week*, July 6, 1998, 16.

victory over an adversary."[22] The U.S. Air Force initially defined IW in 1995 as "any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions."[23] The U.S. military establishment also expanded the concept in the late 1990s, however, to include "information operations" (IO), which refer to "actions taken to affect adversary information or information systems while defending one's own information and information systems."[24]

This conceptual enrichment has also contributed to analytical imprecision. Martin Libicki, a RAND analyst, has identified seven separate categories represented in the myriad discussions of IW: command and control warfare, intelligence-based warfare, electronic warfare, psychological warfare, hacker warfare, economic information warfare, and cyberwarfare.[25]

Pinpointing what they call "InfoWar," Daniel and Julie Ryan argue that:

> Information warfare is, first and foremost, warfare. It is not information terrorism, computer crime, hacking, or commercial or state-sponsored espionage using networks for access to desirable information. These are all interesting and dangerous phenomena ... in today's connected online world, but they are not InfoWar. InfoWar is the application of destructive force on a large scale against information assets and systems, against the computers and networks which support the air traffic control systems, stock transactions, financial records, currency exchanges, Internet communications, telephone switching, credit records, credit card transactions, the space program, the railroad system, the hospital systems that monitor patients and dispense drugs, manufacturing process control systems, newspapers and publishing, the insurance industry, power distribution and utilities, all of which rely heavily on computers.[26]

---

[22]Cited in Winn Schwartau, *Information Warfare: Protecting Your Personal Security in the Electronic Age* (New York: Thunder's Mouth Press, 1996), 12.

[23]Department of the Air Force, *Cornerstones of Information Warfare* (Washington, D.C.: Department of the Air Force Headquarters, 1995), 3-4.

[24]Joint Pub 3-13, *Joint Doctrine for Information Operations* (Washington, D.C.: Joint Staff, October 1998), I-1. Strictly speaking, IW is IO conducted during times of crisis and conflict in order to achieve or promote specific objectives over a specific adversary or adversaries.

[25]Martin C. Libicki, *What is Information Warfare?* (Washington, D.C.: National Defense University Press, 1995), 91.

[26]Daniel J. Ryan and Julie C.H. Ryan, "Protecting the National Information Infrastructure

Table 1
Conventional vs. Information Warfare

	Conventional Warfare	Information Warfare
Battleground	Localized and defined	General and encompassing
Combatants	Well-marked and limited in number	Anonymous, diffuse, and potentially numerous
Targets	Typically military assets (counter-force) or population centers (counter-value); finite	Anything that uses computers or information systems
Offensive advantage favors	Usually the stronger party	The weaker party?
Investments required	Can be prohibitively expensive	More affordable?
Deterrence	Stable	Unstable?

While this admonition helps rectify a common sensationalistic impulse to label everything "war," the definition is too restrictive for our purposes. This paper instead favors a conception of IW that incorporates both this narrow strategic definition and a broader "popular" notion that includes "financial crime, intelligence gathering, and terrorist- and state-based threats"[27]—as long as these acts are used as pseudo-military means to achieve the initiator's political objectives.[28] Table 1 provides a stylized summary of the contrasts between conventional warfare and information warfare.

Viewed from Alger's and Denning's broad concepts, one could argue that human beings have always been concerned with protecting prized in-

against InfoWar," in *Information Warfare: Chaos on the Electronic Superhighway*, ed. Winn Schwartau (New York: Thunder's Mouth Press, 1994), 627.

[27]John I. Alger, "Introduction to Information Warfare," in Schwartau, *Information Warfare* (1994), 12.

[28]Georgetown University scholar Dorothy E. Denning provides a most general definition of information warfare as encompassing "information in any form and transmitted over any media, from people and their physical environments to print to telephones to radio and TV to computers and computer networks." See Dorothy E. Denning, *Information Warfare and Security* (Reading, Mass.: Addison-Wesley, 1999), 12.

formation from adversaries. Denning's illuminating book provides many interesting examples of information warfare throughout human history.[29]

Many label the Persian Gulf War (1991) the first "information war"[30] given that modern information technology played a decisive role. The impressive demonstration of U.S. ability to exploit information convinced many nations that a direct military confrontation with the United States would likely result in defeat. In the 1999 NATO military campaign, the Pentagon successfully launched a cyberattack against Serbia.

The way the United States waged and won these two wars has had a profound impact on nations like China. Art Money, U.S. Assistant Secretary of Defense for command, control, and intelligence, asserts: "The rest of the world realizes that you don't take the U.S. on in a military frontal sense, but you can probably bring it down or cause severe damage in a more oblique way. And that's where the vulnerability in the U.S. resides."[31] Hence, the interesting paradox of asymmetric conflict continues to intrigue.

The "Weapon of the Weak" in Asymmetric War?

One recurring puzzle in international relations is that rather than accepting an objectionable status quo, the weak often take on the strong, thus contravening the canon of deterrence. That such "aberrations" have occurred rather frequently cannot be attributed to either suicidal tendencies or luck on the part of the instigators. This seemingly paradoxical situation needs to be explained.

Thazha V. Paul's pioneering study compared six cases of war initiated by weaker powers and studied the dynamics of asymmetric conflicts.[32] Ivan Arreguin-Toft's more recent article went further by examining the

---

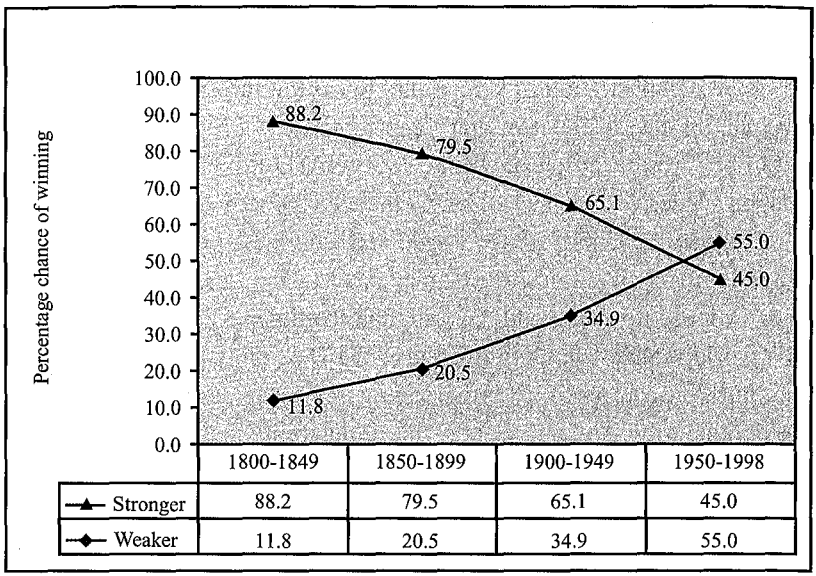
[29]Ibid., 13-16.

[30]Alan D. Campen, ed., *The First Information War* (Fairfax, Va.: AFCEA International Press, 1992), eloquently explained the rationale for this label.

[31]Cited in James Adams, "Virtual Defense," *Foreign Affairs* 80, no. 3 (May/June 2001): 102.

[32]Paul, *Asymmetric Conflicts* (cited in note 3 above).

Figure 1
Does it Pay to Start a Fight?



conditions under which the weaker powers actually won the war.[33]. He found that among all the asymmetric conflicts from 1800 to 1998, the stronger actors won 71 percent of the time whereas the weaker actors won the other 29 percent; this result is consistent with conventional wisdom. What is surprising, however, is that over time the weaker actors won an increasing percentage of asymmetric conflicts. Figure 1 shows how these percentages have changed over four fifty-year periods.

Empirical evidence for the nineteenth century supports the traditional IR dictums favoring the strong in asymmetric conflicts: the weaker actors won only 11.8 percent of the time for 1800-1849, and 20.5 percent for 1850-1899. The weaker actors fared much better during the twentieth century, however, winning 34.9 percent of all asymmetric conflicts for

[33]Arreguin-Toft, "How the Weak Win Wars" (cited in note 3 above).

1900-1949, and 55 percent for 1950-1998. In the most recent period, not only were the weaker actors more prone to initiating conflicts than in previous periods but they were also more likely to win (with the Vietnam War being a prime example). These findings challenge traditional concepts of IR and should, moreover, be of considerable interest to countries like China.

Arrenguin-Toft then analyzes the various scenarios under which strong states can be defeated by their weaker counterparts. He refers to the thinking of Mao Zedong that, when fighting the strong, the weak will benefit from a certain combination of direct and indirect approach strategies. Direct approaches aim at dismantling an adversary's *ability* to fight. Indirect approaches aim at destroying the adversary's *resolve* to fight. He postulates that when strong actors attack with a direct strategy and weak actors defend with an indirect strategy, the weak actor will win. Conversely, when an attack occurs with strong actors using an indirect strategy and weak actors using a direct strategy, the weak actor will also win. In short, when the approaches of both the stronger and the weaker actors converge, the stronger actor is expected to win, but when their approaches diverge, the weaker actor is expected to be victorious.

In both cases the weak actor will come out on top because, either way, the intersection of strategies will prove time-consuming for the stronger actor while the weaker actor will remain resilient. Underlining this idea is the concept of "interest asymmetry" whereby a strong state will be subject to the notion of "relative interest"; because the survival of the strong state is not at stake, it will be less willing to absorb causalities and other losses, while the weak state will make such sacrifices in the name of survival. The relative interest gives rise to "relative political vulnerability" whereby domestic forces will require the strong state to withdraw from a situation where it is suffering significant losses—even though it may have the superior military resources. His model can be summed up as in Figure 2, with the expected winners identified in each cell.

The above historical record and theoretical exposition both show that the notion (and allure) of asymmetric war should not be summarily dismissed as fantasy. Viewed from the standpoint of prospect theory in

Figure 2
Predicting Winners

		Weak-Actor Strategic Approach	
		Direct	*Indirect*
Strong-Actor Strategic Approach	*Direct*	Strong actor	Weak actor
	Indirect	Weak actor	Strong actor

international relations,[34] this analysis shows that the weak actor may overestimate expected gains and underestimate losses by engaging in risk-seeking—rather than risk-averting—behavior. Barry O'Neill cautions that countries might be unable to negotiate their way out of a war because certain kinds of disputes, especially those over symbols or religious places, often generate risk-seeking behavior.[35] Jeffrey Berejekian also finds that states maximize absolute gains whenever possible and always guard against external threats to their sovereignty.[36]

Given both the highly symbolic value and the nonnegotiable status that Taiwan has to the PRC's notion of sovereignty as well as Beijing's oft-repeated warning that it will recover Taiwan at any cost,[37] the PRC may engage in risk-seeking behavior in its military strategy vis-à-vis Taiwan

---

[34]See Jack S. Levy, "Prospect Theory, Rational Choice, and International Relations," *International Studies Quarterly* 41, no. 1 (March 1997): 87-112; Jeffrey Berejekian, "The Gains Debate: Framing State Choice," *American Political Science Review* 91, no. 4 (December 1997): 789-805; and Barry O'Neill, "Risk Aversion in International Relations Theory," *International Studies Quarterly* 45, no. 4 (December 2001): 617-40. For two book-length treatments, see Barbara Farnham, ed., *Avoiding Losses/Taking Risks: Prospect Theory and International Conflict* (Ann Arbor: University of Michigan Press, 1994); and Rose McDermott, *Risk-taking in International Politics: Prospect Theory in American Foreign Policy* (Ann Arbor: University of Michigan Press, 1998).

[35]O'Neill, "Risk Aversion."

[36]Berejekian, "The Gains Debate."

[37]For example, marking the 80th anniversary of the Chinese Communist Party (CCP), Jiang Zemin (江澤民) vowed to some one hundred PLA generals that he would personally lead the PLA into war, and that China would "pay any price" to force Taiwan into Beijing's fold. See "Jiang Pledges to Take Army to War to Liberate Taiwan," Agence France Presse, July 1, 2001 (accessed via *Lexis-Nexus*).

and the United States—especially if it has such instruments as IW. For example, in a veiled threat to destroy U.S. aircraft and ships, prior to the PLA's large-scale military exercises on Dongshan Island (東山島) in July 2001—three months after the midair collision of a U.S. Navy EP-3 surveillance plane with a Chinese fighter, the Chinese military warned that it reserves "the right to resolutely intercept or drive away foreign or Taiwan aircraft or warships conducting reconnaissance. If incoming aircraft or warships refuse to heed the warning, the PLA will open fire to bring them down or sink them."[38] Hence, deterrence as theory and practice may not hold true.

In the context of information warfare, Rattray points out four conditions that are conducive to the waging of a successful strategic IW:[39]

1. *Offensive freedom of action*: Strategic attacks must be able to get through an adversary's defenses and inflict significant damage on chosen targets. Hence, capacity to achieve surprise, speed, and the ability to sustain the vigor of attacks all work to the advantage of the attacker.
2. *Significant vulnerability to attack*: The adversary must possess a vulnerable center of gravity that can be exploited through direct attack, which would erode the political will to fight by destroying the ability of the economy to function, or by disabling the adversary's fielded forces.
3. *Prospects for effective retaliation and escalation are minimized*: A potential attacker must assess its own vulnerability and the likelihood that the adversary would retaliate.
4. *Vulnerabilities can be identified and targeted, and damage can be assessed.*

---

[38]See report by Hong Kong *Wen Wei Po*, citing an article in the July 2001 issue of *Guoji zhanwang* (國際展望), published by the Shanghai Institute of International Studies. Cited from *China Reform Monitor* 397 (July 20, 2001), available online at <http://www.afpc.org/crm/crm397.htm>.

[39]Rattray, *Strategic Warfare in Cyberspace*, 99-100.

Rattray cautions that these enabling conditions are necessary, but not sufficient, for a successful IW. Nevertheless, they unquestionably constitute the elements of any potential serious IW attacker.

The next section shows how the PRC's IW strategies incorporate certain enabling elements in an endeavor to develop "information warfare with Chinese characteristics."

Overcoming the Superior with the Inferior?

China's keen interests in IW should be understood in the context of its security assessment. A Pentagon report states that:

> While seeing opportunity and benefit in interactions with the United States—primarily in terms of trade and technology, Beijing apparently believes that the United States poses a significant long-term challenge. China's leaders have asserted that the United States seeks to maintain a dominant geostrategic position by containing the growth of Chinese power... China has adopted an ambivalent if not skeptical attitude toward the U.S. presence in the Asia-Pacific region.[40]

To spearhead China's military modernization and counter U.S. power, Chinese strategists have explored the potential asymmetric applications of IW for any future conflict with a technologically superior adversary. Although the PRC's current interests in IW appear primarily scholarly, the Chinese military has taken a number of important steps in developing operational IW capabilities: (1) increasing the amount and complexity of IO/IW components in several recent exercises; (2) increasing the PLA's proficiency in defensive measures, most notably against the threat of computer viruses; and (3) recruiting specialists via the PLA's reserve officer selection program by sponsoring the college education of or offering to repay loans after graduation for recruits in return for a military service commitment. The Pentagon report concludes that the PRC has both the capability

[40]Department of Defense, "Annual Report on the Military Power of the People's Republic of China" (July 12, 2002), 8.

to penetrate poorly protected U.S. computer systems and the potential to utilize computer network attacks (CNA) to strike specific U.S. civilian and military infrastructures.[41]

In recent years leading Chinese military journals have published a number of interesting publications discussing IW in the context of "asymmetric warfare."[42] The most notable example is the above-mentioned *Unrestricted Warfare*. In this significant book, the authors propose various tactics useful for developing nations like China to compensate for their military inferiority vis-à-vis the United States. They argue that a digital attack may give China a significant asymmetric advantage and even bring about the defeat of the United States.[43]

Given the Western domination of the discourse on IW, how do the Chinese hope to accomplish these goals? China's approach toward IW fits a pattern that is emblematic of many of its previous reform endeavors —"to retain Chinese teaching as the root and only use Western teaching selectively" (中學爲體西學爲用, *Zhongxue weiti, Xixue weiyong*). In other words, China seeks to develop "information warfare with Chinese characteristics" by integrating traditional Chinese stratagems into modern IW. This strategy poses a challenge to the Western-dominated IW paradigm.

The discourse on IW has traditionally been dominated by the West. Exemplifying the Western paradigm, the Joint Doctrine for Command and Control Warfare (C^2W) defines IW as "actions taken to achieve information

---

[41]Ibid., 31. Admittedly there are other ways to recruit hackers into the PLA, including the commercial front companies employed to build the PLA's networks.

[42]For a *tour d'horizon* of the contending perspectives held by Chinese military thinkers on that country's future security environment, see Michael Pillsbury, *China Debates the Future Security Environment* (Washington, D.C.: National Defense University Press, 2000), esp. chap. 6. For three pioneering syntheses of these articles on IW, translated into English and introduced to the Western audience, see M. Ehsan Ahrari, "U.S. Military Strategic Perspectives on the PRC: New Frontiers of Information-Based War," *Asian Survey* 37, no. 12 (1997): 1163-81; James C. Mulvenon, "The PLA and Information Warfare," in *The People's Liberation Army in the Information Age*, ed. James C. Mulvenon and Richard H. Yang (Santa Monica, Calif.: RAND, 1999), 175-86; and Timothy Thomas, "China's Electronic Strategies," *Military Review*, May-June 2001, 47-54.

[43]Qiao and Wang, *Unrestricted Warfare*.

security by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information-based processes, information systems, and computer-based networks."[44] In practice, however, Western military scholars have been chiefly concerned with offensive IW, especially by targeting the adversary's command and control center in an effort to bring about quick resolution of war.

In military parlance, IW is usually considered an integral aspect of a larger phenomenon known as the RMA. Not merely about technological innovation, RMA also involves the revolutionary impact that technology is having on war-fighting concepts, operational techniques, and organizations. For example, military scholar Andrew Krepinevich writes:

> [A military revolution] occurs when the application of new technologies into a significant number of military systems combines with innovative operational concepts and organizational adaptation in a way that fundamentally alters the character and conduct of conflict. It does so by producing a dramatic increase —often an order of magnitude or greater—in the combat potential and military effectiveness of armed forces.[45]

In this sense, the Chinese armed forces as an institution are undergoing an RMA. The presumed quantum leap in combat effectiveness as a result of RMA constitutes a key impetus for China's forays into IW.

Modern information technology has also created intriguing new possibilities for offensive IW:

> Operations can take place in an instant and come from anywhere in the world. They can be orchestrated and conducted from the comfort of a home or office, without the risks of spies and undercover operations, physical break-ins, and the handling of explosives. The number of targets that potentially could be reached is staggering. Operations could be launched by state or nonstate actors, and by individual groups. The cost to the perpetrators might be negligible, the losses to the victims immeasurable.[46]

---

[44]Ahrari, "U.S. Military Strategic Perspectives on the PRC," 1164.

[45]Andrew F. Krepinevich, "Calvary to Computer: The Pattern of Military Revolutions," *National Interest* 37 (Fall 1994): 30.

[46]Denning, *Information Warfare and Security*, 17.

This quote from IW expert Dorothy Denning shows the ways that IW has altered the nature of war in the information age. First, this type of warfare introduces the intriguing possibility of asymmetric warfare, wherein a weaker actor—in lieu of attacking the stronger party directly—can focus its attack on where the strong party is vulnerable, and is thus able to prevail. The notion of "overcoming the superior with the inferior" resonates with the Chinese, who can draw such inspirations from their rich military history, including Sun Tzu's adage of "winning the battle without fighting" and Mao's "people's war" doctrine. Rather than being obsolete, these traditional stratagems are resurrected to give the Chinese an edge in developing "IW with Chinese characteristics."

Second, IW is quintessentially a form of "unconventional" or "irregular" war. It eschews taking the form of mass armies engaging one another on the battlefield.[47] The anonymity of attackers, the omnipresence of battlefields, the lopsided advantage favoring offense over defense, and the attack that is both of shorter duration and can be automated all make IW a curious weapon of choice by the weak, one that seemingly involves little cost but promises to offer substantial benefit.[48]

For example, *Unrestricted Warfare* promotes expanding combat beyond the battlefield to include such other facets as computer warfare, international terrorism, biological and chemical warfare, and economic and financial warfare.[49] Affirming IW's unconventional character, the book concludes:

> [I]t is precisely the diversity of the means employed that has enlarged the concept of warfare... [T]he enlargement of the concept of warfare has, in turn, re-

---

[47]For an overview of the changing character of warfare, see Martin Van Creveld, *The Transformation of War* (New York: Free Press, 1991).

[48]As articulated by Denning, "Funding a conventional military is not cheap. A single jet can cost a hundred million dollars or more. Then there are ships, tanks, spy satellites, and huge armed forces. By comparison, $1 million to $10 million would amply fund a highly paid IW team of ten to twenty hackers using state-of-the-art computers. The hacking tools themselves can be downloaded without cost from Internet sites all over the world." See *Denning, Information Warfare and Security*, 17.

[49]A caveat is in order: some of the recommendations in this volume, such as state-sponsored terrorism, are fundamentally at odds with the PRC's stated policy.

> sulted in enlargement of the realm of war-related activities.... The battlefield is next to you and the enemy is on the network. Only there is no smell of gunpowder or the odor of blood.... [W]arfare is in the process of transcending the domains of soldiers, military units, and military affairs, and is increasingly becoming a matter for politicians, scientists, and even bankers.[50]

The PRC is interested not in IW per se, but in the strategic and political utility of IW. This holistic approach stems from China's perception of the post-Cold War security environment. China views this U.S.-dominated order (or what Beijing derides as U.S. "hegemonism" and "unilateralism") as threatening the PRC's security interests.[51]

Viewed from power transition theory, today's China—which is experiencing rapid growth and dissatisfied with the existing world order—displays characteristics of an anti-status quo power. A disgruntled rising power may see new technologies, such as IW, as presenting an opportunity to rectify its own disadvantageous security status. This scenario has a negative impact on systemic stability.[52]

Faced with the seemingly invulnerable U.S. military power, smaller and weaker actors have striven to find ways to identify and then penetrate weaknesses in American defense through asymmetric warfare. In this regard, the September 11 terrorist attacks on the United States constitute a form of asymmetric "warfare." IW can be a logical weapon of choice for asymmetric warfare, as such an attack can have a crippling effect on multiple operations and can be undertaken by a militarily and economically disadvantaged state or even by a nonstate actor.

Striving to achieve greater power and prominence on the world stage, the PRC seeks to develop asymmetric IW as a compensation for its inferior

---

[50]Qiao and Wang, *Unrestricted Warfare*, quoted in Bill Gertz, *The China Threat: How the People's Republic Targets America* (Washington, D.C.: Regency, 2000), 16.

[51]The Bush administration's "National Security Strategy" of September 2002 unequivocally states that the United States would use its "position of unparalleled military strength and great economic and political influence" to actively work to "bring the hope of democracy, development, free markets, and free trade to every corner of the world." This document is available online at <http://www.whitehouse.gov/nsc/nss.html>.

[52]See Ronald L. Tammen et al., *Power Transitions: Strategies for the 21st Century* (New York: Chatham House, 2000); and Aaron L. Friedberg, "Ripe for Rivalry: Prospects for Peace in a Multipolar Asia," *International Security* 18, no. 3 (Winter 1993/94): 5-33.

military strength vis-à-vis the United States. True, China almost certainly has the ability to damage inadequately protected U.S. information networks, as pointed out above. The more important question, however, is whether it can use IW as a realistic military option to overcome a superior adversary and still preserve the fruits of its prized economic development, which will surely be destroyed in a retaliation by the adversary. China must think unconventionally about winning the war without fighting, the focus of the next section.

Winning the War without Fighting?

The PLA has come a long way from its revolutionary days in terms of its force structure and doctrines, reflecting its changing security environment and China's changing national priorities.[53] Moving away from "people's war," which sought to compensate for technological deficiencies by pure numerical strength, the PLA's current emphasis is to develop capabilities to fight a "high-tech war" by concentrating on select "pockets of excellence," such as missile and electronic warfare units. IW holds special appeal because many in the PLA count on this strategy to bypass or overcome well-known deficiencies.

Paul Godwin, a PLA expert, asserts that a persistent "doctrine-capability gap" exists for the PLA. He dismisses as obsolete the vast majority of China's ships and aircraft: "They are simply not capable of conducting the kind of war their doctrine envisions: a short, high-intensity conflict fought for limited political objectives within a confined theatre of operations."[54]

---

[53]For a useful overview of the PLA's evolution since 1978, see Dennis Blasko, "PLA Force Structure: A 20-Year Retrospective," in *Seeking Truth from Facts: A Retrospective on Chinese Military Studies in the Post-Mao Era*, ed. James C. Mulvenon and Andrew N.D. Yang (Santa Monica: RAND, 2001), 51-58.

[54]Paul H.B. Godwin, "Compensating for Deficiencies: Doctrinal Evolution in the Chinese People's Liberation Army: 1978-1999," in Mulvenon and Yang, *Seeking Truth from Facts*, 114.

Despite IW's enduring allure for "overcoming the superior with the inferior," implementation is difficult. A PLA paper states that utilization of IW depends not only on sophisticated technology, but also on the integrative use of networked information processes. The central role of information has moved the armed forces toward becoming a network-based organization, integrating the entire military system so that its arms and services can interlink and interact seamlessly. Joint operations, network warfare, and information warfare all are mutually supportive, having tremendous positive—and negative—impacts on the military capabilities of stronger states.[55]

Networked IW represents an intriguing progress whereby moves toward information systems and networks are not only advantageous but increasingly necessary for stronger states. While network-based operations enable enhanced coordination of skilled attacks, a dependence on information can leave the military vulnerable to attacks of its information base, leaving its divisions disintegrated and helpless. Thus strong American information knowledge also exposes a potentially weak side to a determined and increasingly sophisticated adversary.[56]

The Chinese hope to exploit these paradoxes in developing IW in a way that attains Sun Tzu's highest stage of "subduing the enemy without fighting" (不戰而屈人之兵, *buzhan er qu ren zhi bing*). As an example, PLA scholar Su Enze notes that the further information technology develops, the more easily technology can be caught up to, and "the more fungible and vulnerable the information technology becomes."[57] Su's thinking correctly implies that such ironies might be good news for those developing countries seeking shortcuts to technological development.

---

[55]Fang Fenghui, "Grasp the Characteristics of Joint Operations Pertaining to the Time," *Jiefangjun bao* (Liberation Army Daily) (Beijing) (Internet version), June 5, 2001, translated as "Article on Characteristics of Military Joint Operations in Information Age," *FBIS Daily Report: China* (Document no.: FBIS-CHI-2001-0605).

[56]Ironically, as the Chinese C^{4}ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance) system becomes more modernized and computerized, the PRC may also become more vulnerable to American IW methods.

[57]Su Enze, "Logical Concept of Information Warfare," *FBIS Daily Report: China*, June 6, 1996, cited in Ahrari, "U.S. Military Strategic Perspectives on the PRC," 1168-69.

As diffusion of information technology continues apace, American resource advantages in securing information and information systems may gradually erode in relative terms, thus giving rise to hypothetical "windows of opportunity" wherein the field for offense-defense calculation appears temporarily leveled. Recently a PLA author postulated that the advantage is tilting toward the weaker offensive party:

> Information warfare is an all-directional, three-dimensional confrontation. "In offensive, it can infiltrate into every nook and cranny; and in defense, it can stop the infiltration of even one tiny drop of water." In this context, the confrontation between the offensive and the defensive parties are "asymmetrical," and the cost of a reliable defensive system is a lot more than the cost that the offensive side would pay.[58]

The last line evokes similar arguments against missile defense systems: they are expensive and ineffective. However, the author also stresses the importance of defensive IW—which is consistent with Sun Tzu's dictum "knowing the enemy and yourself, you can fight a hundred battles and win them all" (知己知彼百戰百勝, *zhiji zhibi, baizhan baisheng*): "In information warfare, not only must we 'know ourselves and the enemy,' we must, more importantly, make sure that the 'enemy does not have knowledge about us,' and use our knowledge about the enemy to attack the enemy that does not have knowledge about us."[59]

Early Chinese IW discourse was dominated by a focus on the asymmetric advantages that offensive IW presumably gave to the weaker party; recent scholarship on China's underdeveloped IW defense has, however, revealed a gradual maturation of China's IW discourse. Nonetheless, certain concepts of earlier scholarship that focus on gaps (theorized or real) in America's information systems have endured.

The goal of U.S. joint operations (i.e., networking its military around information systems) is the comprehensive integration of units for all mili-

---

[58]Tang Chaojing, "Information Security Plays a Decisive Role in Military Struggles," *Jiefangjun bao* (Internet version), July 17, 2002, translated as "Article Underscores Information Security in Information Warfare," *FBIS Daily Report: China* (Document no.: FBIS-CHI-2002-0718).

[59]Ibid.

tary purposes. By contrast, the goal of Chinese joint operations is the concentration of "capabilities" in a certain direction or zone, with the intention of creating superiority over the enemy in a specific area at a specific time. In an information attack, the PRC hopes to wage asymmetric warfare by crippling a stronger military (e.g., the United States) through the identification and penetration of a gap in the adversary's network and hence overcome the enemy's superior might.[60]

Rather than futilely attempting to match the adversary's comprehensive strength, the Chinese concentrate on exploiting the adversary's weaknesses. PLA joint operations aim to control and prevent the enemy's concentration of joint operations by attacking the enemy's information systems through false or deceptive moves. Such a strategy is aimed at destroying the enemy's capacity to make a decision, leaving the disorganized enemy to be a "host of dragons without a head" (群龍無首, *qunlong wushou*).[61] The Chinese model inspires weak states to explore asymmetric warfare instead of competing directly with strong states.

Michael Pillsbury, an expert on the Chinese military, notes that China is developing other possibilities for asymmetric warfare—the attainment of long-range precision interception weapons, the use of unused frequencies in civilian television and radio broadcasting for information communication, the utilization of encryption-based codes to prevent information stealing, the use of space and satellites to obtain intelligence, the use of saturated tactical ballistic missiles, the development of a directional infrared jamming system, and so on. Chinese military literature also calls for a strategic "reconnaissance" and warning system, a battlefield information network for the promotion of joint operations to better implement asymmetric warfare, and long-range, precision strike systems.[62]

---

[60]Thomas, "China's Electronic Strategies" and Ahrari, "U.S. Military Strategic Perspectives on the PRC" (both cited in note 42 above).

[61]Liu Jun and Zhou Ruhong, "How to Concentrate 'Capability' in Joint Operations," *Jiefangjun bao* (Internet version), June 12, 2001, translated as "PRC Army Paper on Concentrating 'Capability' in Joint Operations," *FBIS Daily Report: China* (Document no.: FBIS-CHI-2001-0612).

[62]For more details, see Pillsbury, *China Debates the Future Security Environment*, chap. 6.

Asymmetric warfare's potential for "subduing the enemy without fighting" intrigues Chinese strategic thinkers. Unlike a traditional, attrition-style war involving battlefield casualties and conquest, a properly executed strategic IW campaign may severely undermine an adversary's ability and willingness to fight. Targets of asymmetric attack can include electrical power grids, civilian aviation systems, transportation networks, seaports and shipping, highways, and television broadcast systems.

Developing IW also dovetails with China's grand strategy of national development. Since 1978 Chinese leaders have been pursuing a fundamental national strategy that seeks to elevate China's overall national power by focusing on economic development. Proponents contend that IW may permit China to compete with the United States militarily, without sacrificing resources designated for economic growth. IW is thus key to China's quest for greatness—on the cheap.

Liu Huaqing (劉華清), the architect of the PLA's modernization, declared at a COSTIND (Commission of Science, Technology, and Industry for National Defense) national conference in 1995 that:

> Information warfare and electronic warfare are of key importance, while fighting on the ground can only serve to exploit the victory. Hence, China is more convinced [than ever] that as far as the PLA is concerned, a military revolution *with information warfare as the core* has reached the stage where efforts must be made to *catch up with and overtake rivals*.[63]

The concept of "overcoming the superior with the inferior" is deeply ingrained in the ethos/mythology of the CCP. Since its revolutionary years, the CCP has had to overcome stronger rivals like the Kuomintang (during the Chinese civil war), the United States (the Korean War), and the Soviet Union (the Sino-Soviet border war). In the past, the PLA made up for a lack of firepower or manpower with superb unconventional or nonmilitary strategies—including guerrilla warfare, psychological trickery, political propaganda, and united fronts. At the dawn of the twenty-first century, however, the PLA feels the need to harness high technology in its struggle against its most probable and powerful strategic rival, the United States. In

[63]Quoted in Mulvenon, "The PLA and Information Warfare," 179. Emphasis added.

developing IW, the Chinese seek to overcome technological deficiencies with superior strategies.

The Persian Gulf War served as a catalyst for the PLA's IW development. Top PLA brass were impressed by superior American technology as well as the destructive power of U.S. joint operations that was created through the "synergy" of multi-service actions, including simultaneous attacks from air force and navy aircrafts, army attack helicopters, and navy strike missiles. In the Gulf War, IW played a key part in helping American military to blind, deafen, and destroy Iraqi forces.

PLA generals realized that the PLA's "people's war" force structure and military doctrine had become anachronistic. They thus have sought to rapidly modernize the military. However, the path they have taken has been fraught with challenges.

Under Deng Xiaoping's (鄧小平) reform programs, military modernization was designated as the last of the Four Modernizations. Consequently, PLA modernization in the late 1970s-early 1990s achieved only modest success, largely due to budgetary limitations.

However, the demise of the Soviet Union, the end of the Cold War, and China's double-digit growth rate in the 1990s have allowed China to substantially increase its military spending and to use its new wealth to acquire advanced weapons and technologies.[64] The PLA is following Deng's advice to develop "selective pockets of excellence."[65] Consequently, IW is playing a very important role in this strategic view of military modernization.

---

[64]Ascertaining the true figures of China's defense expenditure is a matter of considerable debate. In March 2002, Chinese Finance Minister Xiang Huaicheng (項懷誠) announced that China was increasing military spending in 2002 by 17.6 percent, or US$3 billion, bringing the publicly reported total to US$20 billion. However, the publicly disclosed figures do not include major spending for weapons research and foreign arms purchases. A Pentagon report estimates that China's actual military spending could total US$65 billion, making China the second largest defense spender in the world after the United States and the largest defense spender in Asia. See Department of Defense, "Annual Report on the Military Power of the People's Republic of China" (July 12, 2002), 38. The report illustrates the various ways that China has concealed most of its defense modernization spending outside the PLA budget.

[65]Thomas, "China's Electronic Strategies," 48.

As an example of retooling, China has now given its vast 1.5 million-strong reserve force, which in the past was charged with supporting PLA forces in defense against any foreign intervention, with an IW/IO mission. To answer Jiang Zemin's 1991 call for building common telecom systems for both military and civilian use, China's reserve telecom regiments have become the high-tech link under the country's "people's war" theory.[66] Ideas for uniting a "people's war" with IW are finding fertile ground in China's reserve force. Several IW reserve forces have already been formed in Datong (大同), Xiamen (廈門), Shanghai (上海), Echeng (鄂城), and Xi'an (西安). Each is developing its own specialty. Shanghai reserve forces, for example, focus on wireless telecom networks and double-encryption passwords.[67]

East vs. West

If the Chinese IW strategy is not a mere duplication of the Western model, is it an alternative—and superior—strategy? Western and Chinese understandings of information as a mechanism of war vary greatly.

Despite their awe at the American success with the execution of high technology and joint operations during the Gulf War, top PLA generals have resolved not to duplicate American IW; they have instead sought to develop "information warfare with Chinese characteristics."

Summarizing several important Chinese sources on IW, a website maintained by Taiwan's Mainland Affairs Council offers a good introduction to Chinese thinking on IW:

> The so-called information warfare refers to the struggle waged by two opposing sides over the right to acquire, control, and use information.. Such struggles re-

[66]See Zhang Fuyou, "With Joint Efforts Made by Army and People, Military Telecommunications Makes Leap Forward," *Jiefangjun bao*, September 9, 2000. Translated by FBIS, available online at <http://sun3.lib/uci.edu/~scla/microform/resources/f-g/f_049.htm>, quoted in Thomas, "China's Electronic Strategies," 47-48.

[67]Ibid.

> volve around the three basic clusters in the process of information transmission: the source of information, the passage of information, and the recipient of information.... As a broad definition, IW is the use of information technology and methods by the two opposing sides in the political, economic, technological, and military spheres to fight and struggle for an information edge. Viewed from a narrow military standpoint, the contents of IW include the use of both information technology and methods in such military actions as exploring, spying, guidance, command, control, communication, information processing, camouflage and trickery, and strike and killing; military actions aimed to spy on, interfere, destroy, and counter-utilize such actions by the enemy; and countermeasures against the enemy's spying, interference, destruction, and counter-utilization.... The PRC began in the mid-1980s to develop capabilities for next-generation war—called "*dianxue zhanzheng*" (點穴戰爭) or "pinpoint attack" internally, or "information warfare" (信息戰, *xinxi zhan*) from the outside.[68]

The above quote shows that whereas the Western paradigm views information warfare as a series of combat actions taken to attack the enemy's systems of information while preserving one's own information and information systems, the Chinese adopt a more encompassing interpretation of IW, which touches upon the offensive and defensive nature of peacetime, crisis, and war operations, as well as national, strategic, and tactical levels of wartime form.

Western military scholars are concerned with offensive information warfare as it relates to the enemy's command and control center. Chinese authors include elements of electronic, psychological, virtual, and economic warfare, as well as even CNN coverage and the destabilization of

---

[68]"Xinxi zhan ji chaoxian zhan de hanyi tezheng" (Definitions and characteristics of information warfare and unrestricted warfare), available online at <http://www.mac.gov.tw/rpir/2nd1_f.htm>. The concept of "*dianxue zhan*" (點穴戰), sometimes unsatisfactorily translated as "acupuncture war," is a metaphor from many "*wuxia*" (武俠, or *gongfu* 功夫) films or novels, in which certain individuals specialize in finding the critical vulnerable "*xuedao*" (穴道, center of gravity) of the enemy, striking it with a bare finger and causing the enemy to become temporarily paralyzed or lose all his powers. As such, the concept of "*dianxue zhan*" has semblance in the English expression "striking the (almighty enemy's) Achilles' heel." Hence, it is consistent with the notion of asymmetric warfare. The sources used by this website include: "Gaojishu tiaojian xia de xinxi zhan" (Information warfare under high-tech conditions); "Xin zhanzheng lun" (New theories on war); "Chaoxian zhan: Dui quanqiuhua shidai zhanzheng yu zhanfa de xiangding" (Unrestricted warfare: Thoughts on war and art of war in the globalization era); and "Heba: Toushi kuashiji Zhonggong wuli zhuanwen: Dianxue zhan (zixun/xinxi zhan)" (Nuclear hegemon: Thorough investigation into the PRC's military forces in the new century: Entries on acupuncture war [information war]).

financial institutions.[69] The Chinese definition of military science involves not only military operational art but also specific approaches broadly included in military art, such as psychological trickery and stratagems. Western theorists view information as a weapon to be used sparingly and as a mechanism to preserve more conservative structures. Chinese authors interpret information warfare as an *equalizer* through the use of asymmetric and broad-reaching techniques.

Although Chinese concepts of information warfare borrow from the Western idea of information dominance, their methods for achieving information dominance differ. Strategy is important in information warfare. The Chinese see the application of certain ancient stratagems as a way to possess a superior ability to execute strategy and to develop a more complementary military doctrine for force modernization.[70]

It is hard for many to "think outside the box" and realize that America's comprehensive strengths may actually become its weaknesses. This irony, however, is not lost on America's detractors who are seeking to develop isolated "pockets of excellence" and use strategizing to humble the world's surviving superpower. Rather than trying to "catch up" or replicate American methods of information warfare, Chinese IW doctrine emphasizes deception and strategizing—lessons that the American military may take from China on how to exploit this new system of warfare. Through the rise of information warfare, America's comprehensive strength can be a weakness and China's comprehensive weakness may become its strength; this is the type of paradox Chinese military officials have long recognized and sought to exploit.

Although the United States demonstrated its IW prowess in the Gulf War, its military strategy is not flawless. As information weapons and tech-

---

[69]Ahrari, "U.S. Military Strategic Perspectives on the PRC," 1164.

[70]Chinese IW strategies revitalize the execution of the classic *Thirty-Six Strategies: The Secret Art of War*. Timothy Thomas, an American military analyst, argues that there are clear IW connections to the first five strategies—in which information creates an environment of anonymity, ambiguity, and the chaos/confusion of ethical retaliation—that the Chinese have long dominated traditionally. See Thomas, "China's Electronic Strategies." An English translation of the *Thirty-Six Strategies* of ancient China is online at <http://www.chinastrategies.com>.

nologies drive joint operations, such network-based information systems become highly vulnerable to asymmetric attack. While U.S. strength lies in technological and strategic mechanisms for information, their movements leave significant network gaps open for asymmetric attack, granting the PRC space to exercise its strong suit—asymmetric tactics.

The PRC has more experience (and success) with asymmetric warfare than the United States. While the United States currently leads the PRC in information technologies and resources, the potential threat from the PRC cannot be dismissed. Chinese military history celebrates techniques of asymmetric warfare, and the Chinese interpretation of warfare is also far more encompassing than a traditional Western view. This entails a potentially far greater scope of destruction—entering the private, civilian spheres as well. While waging IW against the United States may still be many years off, the PRC has shown keen interest in integrating IW in its overall military strategy vis-à-vis Taiwan.

The New Factor in Cross-Strait Military Calculus

The advent of IW has introduced a new element into the cross-Strait military situation by presenting China with a potentially credible military option vis-à-vis Taiwan.

A Pentagon report states that despite Beijing's professed commitment to a peaceful unification with Taiwan, the Chinese leadership has shown an increasing willingness to consider the use of force to achieve unification. The report surmises that "Beijing's primary political objective in any Taiwan-related crisis ... likely would be to compel Taiwan authorities to enter into negotiations on Beijing's terms and to undertake operations with enough rapidity to preclude third-party intervention."[71] The report also seems to concur with the view of some analysts that the PLA's of-

[71]Department of Defense, "Annual Report on the Military Power of the People's Republic of China" (July 12, 2002), 46.

fensive capabilities improve as each year passes, providing Beijing with an increasing number of credible options to intimidate or actually attack Taiwan.[72] With the exception of ballistic missiles, IW seems the most promising option for achieving Beijing's political objectives. Indeed, the PRC has made considerable efforts toward making IW a real option.

Certain PLA officers have promoted IW as an effective weapon to subdue Taiwan and to deter possible American intervention. Articles written by several strategists at the Jinan Military Region (濟南軍區), collected in a volume on IW published by the PLA's National Defense University Press in 1999, discussed the roles of IW in a combined amphibious battle. They illustrated the main forms that IW can be waged under such a campaign:[73]

1. *Command and control war*: To degrade and destroy the enemy's anti-landing command and control systems.
2. *Intelligence war*: To acquire the intelligence needed for a successful amphibious campaign will take place in all domains, including land, sea, sky, space, and electromagnetics.
3. *Network war*: To gain control and damage the enemy's computer network systems by adhering to three priorities: (a) comprehensively paralyzing the enemy's network systems; (b) flexibly employing attack methods; and (c) training and using "cyber-warriors" (hackers), including the establishment of a special cyber-force with expertise in computer know-how and advanced decoding techniques.
4. *Communication war*: To destroy the "nerve" of the enemy's command and control systems; and

---

[72]Ibid., 47. Representing this view is David Shambaugh, "A Matter of Time: Taiwan's Eroding Military Advantage," *The Washington Quarterly* 23, no. 3 (Spring 2000): 119-33.

[73]Liu Yuhua et al., "Lianhe dengdao zhanyi xinxi zuozhan wenti yanjiu" (A study on the information warfare issues involved in a combined landing battle), in *Wojun xinxizhan wenti yanjiu* (A study on the issues of our military's information warfare) (Beijing: National Defense University Press, 1999), 209-16.

5. *Electronic war*: To weaken and destroy the enemy's electronic equipment.

The Chinese military has begun to put these ideas into practice. In the summer of 2001, the PLA for the first time began the war game exercises in the Taiwan Strait with information warfare aimed at electronically paralyzing enemy communications and command systems. Also for the first time, a new electronic warfare unit was deployed over the Strait.[74] In exercises the following year, the PLA incorporated even more sophisticated items of IO/IW.

In sum, the PLA seeks to gain information domination in any conflict with Taiwan by attacking Taiwan's information networks and command and control centers, as well as by conducting propaganda and political warfare. The purpose is to incorporate Taiwan by "subduing the enemy without actually fighting" à la Sun Tzu, and by denying possible American military intervention.

This trend presents a new challenge to Taiwan and U.S. defense officials. Most analysts have hitherto: (1) dismissed Chinese invasion threat due to the high threshold for success (due to logistical difficulties, Taiwanese resistance, and international intervention); (2) argued that Taiwan's smaller military can maintain a qualitative edge until at least 2005; (3) questioned whether Beijing has realistic military options vis-à-vis Taiwan despite both the PRC's consistent refusal to renounce the use of force and occasional saber-rattling against Taiwan; and (4) held that a probable, albeit not guaranteed, U.S. military intervention (in the case of an unprovoked attack on Taiwan) serves to deter Beijing—i.e., the so-called policy of strategic ambiguity.

From the Chinese standpoint, IW seems to have lowered the threshold for a likely successful military campaign against Taiwan and increased the utility of an offensive strategy. IW seems to hold promise for "winning the

[74]Craig S. Smith, "Beijing Stages War Games, Mostly for Taiwan," *The New York Times*, July 10, 2001, A6; and Vincent Wei-cheng Wang, "'Information Warfare' Changes Taiwan Equation," *The Washington Times*, July 13, 2001, A18.

battle without fighting" (Sun Tzu's adage) and "overcoming the superior with the inferior" (Mao's guerrilla strategy). Properly executed IW may—along with such other coercive weapons as missile strikes and a naval blockade—help bring Taiwan to its knees and deny American intervention. Such perceptions may cloud decision-making and make China more likely to use force. The application of information technology in international conflicts such as cross-Strait tensions may thus result in more instability.

Curiously enough, however, some sort of deterrence is emerging in the field of IW. The perceived advantage IW has in terms of offense will only hold true if the adversary fails to take proper countermeasures to augment its own offensive and defensive IW capabilities. For example, after then-President Lee Teng-hui (李登輝) stated his "state-to-state" theory in July 1999, hundreds of Chinese hackers attacked Taiwanese web servers—which in turn led to retaliation by Taiwanese hackers.

After the midair collision between an American Navy EP-3 plane and a Chinese fighter in April 2001, a self-styled Honker's Union[75] utilized modern information technology via their website, e-mail system, and downloadable viruses to recruit fellow patriots in a "people's war" against the United States by attacking thousands of American websites. Their attacks triggered a furious retaliation by hackers based in the United States.[76]

These early glimpses into cross-Strait "cyberwar" show that in IW, the emphasis on the advantage of offense should be balanced by reflection on the importance of defense. At least for now, the PRC cannot launch IW without suffering reprisal. Hence, a curious digital "mutual assured destruction" (MAD) is emerging. State-sponsored hacking is unlikely to fundamentally alter the international power structure. Indeed, the Chinese government in May 2002 asked private hackers not to repeat the defacement of U.S. government websites that had occurred a year ago, according

---

[75]The group's name in Chinese means "Red hackers" (紅客, *hongke*), indicating the *political* motives for their actions.

[76]For more details on these two episodes, see Vincent Wei-cheng Wang and Gwendolyn Stamper, "Asymmetric War? Implications of China's Information Warfare Strategies," *American Asian Review* 20, no. 4 (December 2002): 199-202.

to Air Force Major General John Bradley, deputy commander of the Pentagon's Joint Task Force on Computer Network Operations.[77] This shows a sobering of China's IW endeavor.

To counter China's IW development, Taiwan has undertaken its own forays into IW. In the summer of 2001, Taiwan's military established its own electronic-warfare unit.[78] In June 2002, Taiwan for the first time incorporated a new facet into its decades-old Wan'an (萬安) air-raid drill to boost the island's Internet defenses against hacker attacks, especially from China.[79] A White Paper released by Taiwan's Defense Ministry in July 2002 states that a three-pronged defense strategy was envisaged in the face of increasing threats from China's military satellites, ballistic missile technology, and information warfare: (1) to prevent war by building a sustainable defense capability so that "the enemy dare not rashly wage a war"; (2) to maintain stability in the Taiwan Strait through dialogue between the two sides on security issues; and (3) to ensure the island is ready to defend itself in the event of an invasion.[80]

The White Paper notes China's expanding military power—including the PLA's efforts to acquire capabilities related to space, electronic, information, and precision attack warfare—which would enable the Chinese military to conduct a first strike against Taiwan. In response, the White Paper calls for Taiwan to build a "compact but delicate, highly capable" modern force by reducing the number yet increasing the quality of personnel and strengthening technological capability. Included in the deterrence strategy are: establishing an early warning system, building offensive and defensive capabilities to conduct information and electronic operations,

---

[77]Cited in Pamela Hess, "China Prevented Repeat Cyber Attack on U.S.," UPI, October 29, 2002, from *The Washington Times* (<http://www.washtimes.com/upi-breaking/20021029-121924-5101rhtm>).

[78]Brian Hsu, "Army Forms Its First Electronic-Warfare Unit," *Taipei Times*, July 31, 2001, available online at <http://www.taipeitimes.com/news/2001/07/31/print/0000096461>.

[79]"Web 'Drill' to Tackle Hackers," *The Australian*, April 30, 2002, C2 (from AFP wire) (accessed via *Lexis-Nexus*).

[80]Goh Sui Noi, "Taiwan's Strategy: To Deter and Build Trust; a White Paper Outlines the Island's Strategy to Build 'Sustainable Defense' to Prevent a Possible Invasion by China," *The Straits Times*, July 24, 2002 (accessed via *Lexis-Nexus*).

and maintaining air superiority and naval dominance.

The PRC's IW development has introduced uncertainties and risks into this volatile region that cannot be overcome until a stable "digital MAD" of some sort is established in the Taiwan Strait. This is a case of how technology, combined with intentions and (mis-)perceptions, may become a destabilizing factor. IW may tempt PLA commanders to launch a preemptive strike. China's design for Taiwan is most likely to be a short, decisive blow that results in Taipei's capitulation: i.e., a *fait accompli* presented to the international community. This is much preferred by Beijing to a protracted campaign, such as an amphibious invasion or embargo that could invite an uncertain response from other actors. IW appears especially attractive in this regard, promising both a quick resolution of the military contingency and a low casualty rate, so as to preserve Taiwan's industrial and commercial assets for Beijing.

An Emergent Threat?

How seriously should Taiwan and American defense planners take the PRC's IW endeavors? There is no question that the Chinese military is keenly interested in studying IW. At the present moment the PLA's interest is primarily academic; its IW capabilities are far from operational (weaponized). One can safely say that at the present time the modernization of the Chinese armed forces has lagged behind doctrinal development.

Nevertheless, China's IW forays will benefit from two factors—one old and one new. Historically, China has more than once surprised Western analysts by indigenously developing weapons systems that the West tried hard to deny to China (e.g., atomic bombs in 1964 and nuclear warhead miniaturization technology in 1999). Prudence thus cautions against dismissing the possibility that China may succeed in developing "IW with Chinese characteristics." Whether a modern IW doctrine guided by proven historical stratagems will surpass the Western model remains to be seen, however.

Most importantly, the future of China's IW development hinges on

Table 2
Growth of Online Populations in Select Countries

Unit: Millions

	China	Taiwan	India	Japan	U.S.
1997	0.2 (June 1997)	1.1	0.2 (Nov. 1997)	10.0 (Oct. 1997)	56.0 (Nov. 1997)
1998	1.5	2.8 (Sep. 1998)	0.5 (Nov. 1998)	14.0 (Oct. 1998)	73.0 (Oct. 1998)
1999	7.0	4.8	0.8 (May 1999)	19.5	106.3 (July 1999)
2000	22.5	6.4 (July 2000)	5.0	47.1	164.4
2001	26.5 (July 2001)	11.6 (July 2001)	7.0	49.4 (Jan. 2001)	166.1 (Aug. 2001)
2002	45.8 (July 2002)	N/A	N/A	56.0 (June 2002)	165.8 (April 2002)
% of population (latest figures)	**3.58%**	**51.8%**	**0.67%**	**44.1%**	**59.10%**
Ranking among 62 countries	**51**	**34**	**56**	**35**	**11**

Note: Year-end figures, unless otherwise noted.

Sources: "NUA Internet: How Many Online," at <http://www.nua.com/surveys/how_many_online/asia.html> and <http://www.nua.com/surveys/how many online/n america.html>; and "Measuring Globalization: Who's Up, Who's Down," *Foreign Policy*, January/February 2003, 65.

the country's economic ascendancy in general and its rise as a major global IT player in particular. Thanks in large measure to investments by Taiwanese IT firms on the mainland, the PRC has recently overtaken Taiwan as the world's third largest IT hardware producer and is poised to overtake Japan in the next decade if current growth trends continue. In addition, China's online population is experiencing exponential growth: from 200,000 in 1997, to 16.9 million in July 2000, and to 45.8 million in July 2002, making China one of the largest and fastest-growing Internet markets.[81] Table 2 shows the low base and fast growth of China's online popu-

[81]"NUA Internet: How Many Online," at <http://www.nua.ie/surveys/how_many_online/asia.html>.

lation, in comparison with select countries.

It should be noted that viewed from another measure of information power—Internet penetration rate (i.e., online population as a percentage of total population), China remains sparsely wired. As of July 2002, only 3.58 percent of its population was online, up from 0.001 percent six years ago. Compared to the United States, Japan, and even Taiwan, China clearly has a long way to go before it can claim to be a true information power. Table 2 also shows that on the Globalization Index compiled by *Foreign Policy* and A.T. Kearney,[82] China also pales in comparison, edging out only India.

China's mixed record as an IT society in an increasingly globalized economy—i.e., being a giant in absolute terms and with tremendous upside potential, while also being a dwarf in relative terms—will affect the degree of success of China's further inroads in IW. The PLA's immersion in both IW and RMA is understandable. However, it is hard to imagine a superb IW fighting force detached from a society characterized by relatively low technology and connectivity.[83] A strong IT base gives rise to a strong IW capability. The PLA may thus continue facing difficulties in surmounting the military's acknowledged doctrinal-capability gap.

The flip side of this argument is that Taiwan's security depends on a strong and continuously improving IT sector. This is because the IT sector has vital links to other sectors and is vital to overall economic development. A second factor is that the IW "arms race" across the Taiwan Strait has already begun. The increasing number and sophistication of Taiwanese IT firms investing in China has thus created politico-military externalities, apart from the economically beneficial decisions to relocate to the mainland given globalization-induced pressures. The broader implications of these trends require further investigation.

---

[82]This index is a composite ranking of sixty-two of the world's most globalized economies based on thirteen indicators grouped into four categories: political engagement, technology, personal contact, and economic integration. See "Measuring Globalization: Who's Up, Who's Down," *Foreign Policy*, January/February 2003, 60-72.

[83]Taiwan's conscription system and the island's widespread online population mean that the military can choose from a tech-savvy population to find capable hackers.

Issues & Studies

An International Quarterly on China, Taiwan, and East Asian Affairs

INTERNSHIP OPPORTUNITY

Issues & Studies is pleased to offer an internship opportunity in our editorial department. Applicants should be a graduate student in a social science department, be a native English language-speaker, and preferably have research experience in issues related to China, Taiwan, or East Asia.

This unpaid internship is on a semester-basis (fall/spring/summer), with free room & board as well as office, computer, and internet access provided in exchange for part-time help in various duties related to journal publishing.

Interested candidates should contact Andrew D. Marble, *Issues & Studies* Deputy Managing Editor, at **<adm@ms2.seeder.net>**.

Institute of International Relations (IIR)
Taipei, Taiwan (ROC)