Asymmetric War? Implications for China's Information Warfare Strategies

Vincent Wei-cheng Wang  
University of Richmond, vwang@richmond.edu

Gwendolyn Stamper

Follow this and additional works at: http://scholarship.richmond.edu/polisci-faculty-publications

Part of the Defense and Security Studies Commons, International Relations Commons, and the Military and Veterans Studies Commons

Recommended Citation

ASYMMETRIC WAR?
IMPLICATIONS FOR CHINA'S INFORMATION
WARFARE STRATEGIES

Vincent Wei-cheng Wang and Gwendolyn Stamper*
University of Richmond

Abstract

This essay discusses the emerging discourse and capability of the PRC on information warfare (IW) and the implications of such developments on cross-Strait and US-PRC relations. It finds that the PRC’s endeavors in IW stem from the conviction among certain well-informed writers in the PLA that IW occupies a crucial place for a Revolution in Military Affairs (RMA) in China’s military modernization. Chinese strategists explore IW’s potential for China to wage an “asymmetric war” (defined as the use of surprise force by a weaker party against a stronger but vulnerable adversary) by applying traditional strategems (e.g., Sun Tzu’s “overcoming the superior with the inferior” and Mao’s “people’s war”) in modern warfare. Chinese strategists argue that IW can help China counter overall American strengths by targeting certain “pockets of excellence,” rather than attempting to match America’s comprehensive power, and present China with a credible military option.

* The authors acknowledge the support for this project from a University of Richmond faculty-student collaborative research grant and the comments of an anonymous reviewer of the American Asian Review. A version of this paper was presented at the 2002 annual meeting of the American Political Science Association.
for achieving its political objective of achieving unification with Taiwan (on Beijing's terms) through deception, surprise, and decisiveness. These strategic considerations can introduce instability in the Taiwan Strait region. They also raise questions about certain conventional aphorisms in international relations. The evolution of Chinese military doctrine and force structure is traced. Chinese and American concepts of IW are contrasted. Early examples of "cyberwar" between China and the US and between China and Taiwan are examined. The article concludes with a cautionary note on an emergent "digital mutual assured destruction."

Know thy enemy, know yourself, your victory will never be endangered.

–Sun Tzu, *The Art of War*

. . .warfare which transcends all boundaries and limits – in short, unrestricted warfare.

–Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*

Two aphorisms have been widely and uncritically accepted by most security scholars and analysts: 1) in a conflict, the party with preponderant force prevails – either in coercing the weaker party to take an action desired by the former (compel-lance) or in dissuading the weaker party from taking an action detested by the former (deterrence); and 2) although the People's Republic of China (PRC) has refused to renounce the

---


use of force against Taiwan, it currently has few credible military options.

This article examines the emerging discourse and capability of the PRC on information warfare (IW) and discusses the implications of these developments on cross-Strait and US-PRC-Taiwan relations. It argues that the PRC’s endeavor in IW stems from the belief among certain well-read writers within its military (the People’s Liberation Army or PLA) that IW occupies a crucial place in a Revolution in Military Affairs (RMA) in China’s military modernization. These authors seem particularly keen on the potential IW holds for China to apply traditional stratagems (e.g., Sun Tzu’s “overcoming the superior with the inferior” and Mao’s “people’s war”) in modern warfare in order to wage an “asymmetric war” – defined as the use of surprise force by a weaker party against a stronger force’s vulnerability.3

Moreover, these analysts think that IW can present a credible military option for the PRC to reincorporate Taiwan on Beijing’s terms and to deter the US from intervening in the cross-Strait conflict. The July 12, 2002 Pentagon report to Congress 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.4 The report further 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

---


4 Department of State, “China is Considering a Coercive Strategy on Taiwan, DOD Says,” e-mail update sent by IIP Dept. of State <schinapd@YAHOO.COM> to <US-CHINA@LIST.STATE.GOV> July 16, 2002.
adversary.”

For these reasons, a study of China’s IW strategies is timely and important. This study also poses a challenge to the two aphorisms posited at the outset.

IW, The Future War?

In recent years, there has been an increasing recognition of the importance of information technology (IT) on conflict. Although “cyberterrorism” certainly presents a frightening prospect for “the next war” because various state and nonstate actors may manage to eventually possess the technological skills or opportunities to engage in extremely damaging netwar, this is by no means the only dangerous implication of the information revolution. As three experts prophetically wrote, this revolution is enabling new forms of organization and new doctrines that will affect the spectrum of conflict, including terrorism.

While Americans still are grappling with the surprise, deception, and shock created by the September 11, 2001 terrorist attacks, some analysts caution about the prospect of weaker parties engaging in IW or cyberterrorism against the United States or other democracies. This is because in the US, it is the private sector, namely those numerous companies whose main motive is profit, that control computer networks, whereas defending national security falls under the purview of the military.

---


In his testimony to the Senate Arms Services Committee on March 9, 1999, Deputy Secretary of Defense John Hamre said that, although the Pentagon thought it had done a good job of protecting national security from hackers, he was worried about the vulnerability of commercial and financial interests. "And this (electronic) Pearl Harbor's going to be different," Hamre warned. "It's not going to be against Navy ships sitting in a Navy shipyard; it's going to be against commercial infrastructure, and we don't control that. And there has been little progress on that."\(^8\)

Hamre's concern shows that America's very strength – openness and accessibility of information – could turn into its Achilles' Heel, if an adversary can exploit it. The wide diffusion of computers worldwide and interconnectedness of information networks convince James Adams, the brainchild of iDefense, a company that aspires to be "the Central Intelligence Agency for the private sector," 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.\(^9\) This fact lets some weaker parties with grievances contemplate that they can take on stronger parties and perhaps even prevail in an "asymmetric conflict." This trend could be destabilizing.\(^10\)

Defense expert Dan Kuehl of National Defense University lists China, Russia, Iraq, Libya, terrorist groups like Osama bin Laden's Al-Qaeda, and even unsavory organizations in friendly nations as "cyberthreats."\(^11\) In his testimony to the

---


\(^9\) James Adams gives an exhaustive history of information warfare, as well as the US military's capabilities, stating categorically that the Air Force can track hackers back to their computers and launch "computer bombs." However, many of America's enemies also have the same skills. See James Adams, *The Next World War* (New York: Simon & Schuster, 1998).


\(^11\) Galvin, "Info War," 72.
Senate Government Affairs Committee on June 24, 1998, CIA director George Tenet told lawmakers that intrusion into government computers will become increasingly more sophisticated and better organized and is likely to involve hostile nations. "Potential attackers range from national intelligence and military organizations, terrorists, criminals, industrial competitors, hackers and disgruntled or disloyal insiders." He further said, "We know with specificity of several nations that are working on developing an information warfare capability."^12

In light of the perceived technological superiority of the military of the United States, the PRC appears keen on pursuing IO/IW development as a key part of its overall military modernization and concomitantly exploring IW as an alternative way to counter US power. The Pentagon report analyzes China’s security assessment:

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. ... Most importantly, China has adopted an ambivalent if not skeptical attitude toward the U.S. presence in the Asia-Pacific region.^13

As the article will show, Chinese strategists have devoted considerable interests to exploring the potential asymmetric applications that IO/IW can have in a future conflict with a technologically superior adversary. The Pentagon report lists

^12 While Tenet did not identify the countries, committee chairman Fred Thompson (R-Tenn), who received a classified briefing a day before, named some of them. Citing published reports, Thompson said that China, Russia, Libya, Iraq, Iran, and at least seven other countries were developing IW programs. See “CIA Director Warns of Intrusion into Government Computers,” Associated Press, June 24, 1998, accessed from Lexis-Nexis, and Jennifer Mateyaschuk, “Nothing to Raise A Glass About,” Information Week, July 6, 1998, 16.

some of the endeavors beyond scholarly discussions by the PRC to develop IW capabilities such as:

- Increasing the amount and complexity of IO/IW components in several recent exercises,
- Increasing the PLA's proficiency in defensive measures, most notably, against the threat of computer virus, and
- Recruiting specialists via the PLA's reserve officer selection program, by sponsoring the college education of students or offering to repay loans after graduation in return for a military service commitment.

The report concludes that the PRC has the capability to penetrate poorly protected US computer systems and potentially use computer network attack (CAN) to strike specific US civilian and military infrastructures.15

This article shows that China's approaches to IW pose fundamental challenges to certain conventional maxims of international politics and raise important questions about national security. These questions confirm the growing salience of technology in international relations and necessitate a fresh understanding of the nature of war.

The transitions to an information age and the shifts from the industrial age to the postindustrial age have caused many analysts to proclaim that "technology transforms world politics"16 and "information is power."17 However, a full grasp of

---

14 Drawing on Sun Tzu's adage, "Knowing the enemy and yourself, you can fight a hundred battles and win them all," a recent PLA Daily article makes the case that preserving information security is extremely important. "In information warfare, not only must we 'know ourselves and the enemy,' we must, more importantly, make sure that the 'enemy does not have the knowledge about us,' and use our knowledge about the enemy to attack the enemy that does not have knowledge about us." See Tang, Chaojing, "Information Security Plays a Decisive Role in Military Struggles," Beijing Jiefangjun Bao (Internet version) July 17, 2002, translated as "Article Underscores Information Security in Information Warfare," FBIS Daily Report: China (Document Number: FBIS-CHI-2002-0718).


16 Jeffrey R. Cooper, "Another View of Information Warfare: Conflict in
the effects of information technology on interstate conflict remains elusive. What Robert Keohane and Joseph Nye call a “new conventional wisdom” holds that the information revolution has a leveling effect, promising to enhance the power of weak state and nonstate actors vis-à-vis that of powerful ones.

However, many dispute the “advantage to the weak” argument, contending that the notion of “asymmetric conflict” sounds appealing but is not feasible. An exploration of this issue should begin with an understanding of the basic concepts.

John Alger, an IW expert, argues that 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 victory over an adversary.”18 If we follow Alger’s definition, we can argue that human beings always have been concerned with protecting prized information from adversaries. Numerous examples of information warfare can be found throughout human history.19

However, it was not until the Persian Gulf War (1991) that the decisive role of modern information technology in warfare became indisputably clear. The impressive demonstration of the ability of the US to exploit information convinced many nations that a direct military confrontation with the US likely would result in defeat. In the 1999 NATO military campaign,
the Pentagon successfully launched a cyberattack against Serbia.

America's military successes have inspired countries like China to avidly study and develop IW in an effort to counter US power and to explore ways to gain an asymmetric advantage vis-à-vis the US. Art Money, 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."20

In recent months, leading Chinese military journals have published a number of noteworthy articles discussing IW in the context of "asymmetric warfare."21 The most notable example is Unrestricted Warfare, written by two PLA colonels in early 1999. In this potentially very significant book, the authors propose various tactics for developing countries such as China to compensate for their military inferiority vis-à-vis the US. They argue that a digital attack may give China a significant asymmetric advantage and even bring about the defeat of the US.22

In this article, China's IW doctrine and capability is examined. The focus is on the political objectives of China's


22 Qiao and Wang, Unrestricted Warfare.
Information Warfare: The New Weapon of the Weak?

The discourse on IW has been dominated by the West. This article argues that Eastern and Western notions of IW share varying limitations regarding the scope and intention of IW use. As an example typifying the Western perspective, the Joint Doctrine for Command and Control Warfare (C2W) defines information warfare as "actions taken to achieve information 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."\(^{23}\)

---

\(^{23}\) Ahrari, "U.S. Military Strategic Perspectives on the PRC," 1164.
Traditionally, Western military scholars have been concerned mainly with offensive IW as a mechanism to attack increasingly dependent information processes and systems. IW focuses on specific attacks of the adversary’s command and control center through the use of smaller force and more sophisticated technology, bringing an end to multiyear, attrition-oriented battles. IW focuses not only on the possession of advanced technologies, but also on mechanisms of integration, designing effective “synergies” to rapidly coordinate the otherwise fragmented military for home network defense as well as the invasion of foreign information system. The scope of IW differs both individually and culturally, and can invade both the private and civilian spheres of everyday life.

Made possible by technological advances in communication and computation, IW is an integral aspect of a larger phenomenon that is generally known as the “evolution in Military Affairs (RMA).” As M. Ehsan Ahrari points out, recent discussions on RMA have shifted from a narrow focus on technology to the consideration of the revolutionary impact technology will have on war fighting concepts, operational techniques, and organizations. Describing RMA, 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.24

Following this definition, some analysts, such as Ahrari, argue that the Chinese armed forces as an institution are undergoing an RMA. The supposed quantum leap in combat

effectiveness as a result of RMA is a major rationale for China’s IW development.

However, at a more general level, modern information technology likewise has created many new possibilities for offensive IW, as pointed out by Denning:

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.25

Denning’s description illustrates the several important ways that IW has altered the nature of war in the information era. First, it introduces the intriguing possibility of asymmetric warfare, defined as a military strategy by the weaker actor to not attack the stronger party directly, but to focus its attack on where the strong party is vulnerable and then to prevail. The Chinese reason that the traditional notion of “overcoming the superior with the inferior,” which draws inspiration from Sun Tzu’s adage of “winning the battle without fighting” and Mao’s “People’s War” doctrine, rather than being obsolete, might give them an edge in developing IW. Asymmetric warfare challenges the traditional realist and neorealist schools by redefining power (offense-defense calculations), and by rendering the outcome of international conflict more indeterminate.

Second, IW is an epitome of what is often called “unconventional” or “irregular” conflict. It does not take the form of mass armies engaging one another on the battlefield, or the traditional air- or sea-based military operations in support of

such engagement.\textsuperscript{26} The anonymity of attackers, the omnipresence of battlefields, the lopsided advantage favoring offense over defense, and the attack that is of shorter duration and can be automated make IW a curious weapon of choice by the weak, one that seemingly involves little cost but promises to reap substantial benefit.\textsuperscript{27}

The authors of \textit{Unrestricted Warfare} advocate expanding combat beyond the battlefields to include computer warfare, international terrorism, biological and chemical warfare, economic and financial warfare, and more. Their views clearly affirm IW's unconventional character:

\begin{quote}
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.\textsuperscript{28}
\end{quote}

The authors conclude:

\begin{quote}
Clearly, it is precisely the diversity of the means employed that has enlarged the concept of warfare. Moreover, the enlargement of the concept of warfare, has, in turn, resulted 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. . . . Obviously warfare 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.\textsuperscript{29}
\end{quote}

\textsuperscript{26} For an overview of the changing character of warfare, see Martin Van Creveld, \textit{The Transformation of War} (New York: Free Press, 1991).

\textsuperscript{27} As Denning puts it, "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 20 hackers using state-of-the-art computers. The hacking tools themselves can be downloaded without cost from Internet sites all over the world." \textit{Information Warfare and Security}, 17.

\textsuperscript{28} Qiao and Wang, \textit{Unrestricted Warfare}, quoted in Adams, "Virtual Defense," 103.

\textsuperscript{29} Qiao and Wang, \textit{Unrestricted Warfare}, quoted in Bill Gertz, \textit{The China
In a larger strategic context, the PRC’s interest in IW and other forms of asymmetric warfare stems from its perception of the post-Cold War security environment. Most Chinese view what they call American “hegemonism” and “unilateralism” that is buttressed by America’s military power as the main threat to China’s security interests. The demise of the Soviet Union left the US the unchallenged military superpower in a new and ambiguous unipolar power structure. Emerging political and economic tensions have caused certain dissatisfied states to search for a tool through which to express their increasing frustration. Recognizing the virtually impregnable forces of the comprehensive American power, smaller and militarily inferior actors increasingly have been drawn to find ways to isolate and penetrate weaknesses in American defense through the use of asymmetric warfare. Viewed in this context, the September 11 terrorist attacks on the US constitute a form of asymmetric “warfare.”

In many ways, information warfare lends itself to the exploitation of asymmetric conflict, as such an attack 1) can have a crippling effect on multiple operations, and 2) can be done by a militarily and economically disadvantaged state or even nonstate actor. As the PRC strives to become an international superpower, asymmetric IW serves as compensation for its inferior military strength relative to American force. The PRC cannot match superior American military technology. However, IW presents possibilities for the PRC to match the US in other ways, such as damaging less protected information networks, where America’s overall strengths lie.


The PRC’s love affair with asymmetric warfare evolves from a distinctive Maoist doctrine of people’s war that stresses numeric strength over technological prowess. The next section surveys the PRC’s changing doctrine and force structure.

**From People’s War to High-Tech War**

The PRC’s current foray into IW reveals the protracted evolution of its doctrine and force structure since the “people’s war” of its early years. Figure 1 distinguishes four stages, 1) People’s War, 2) People’s War under Modern Conditions, 3) Local War, and 4) Local War under Modern High-Technology Conditions, and summarizes the changing relationship of PLA doctrinal development to force structure.

---

**Figure 1: China’s Evolving Military Doctrine**

<table>
<thead>
<tr>
<th>Force structure</th>
<th>PW</th>
<th>PWUMC</th>
<th>LW</th>
<th>LWUMHTC</th>
<th>RMA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single service operations; filed armies</td>
<td>Joint headquarters / operations; group armies</td>
<td>Fist units, rapid reaction units</td>
<td>Smaller and fewer units; more high-tech</td>
<td>Selective pockets of excellence?</td>
<td></td>
</tr>
</tbody>
</table>

| Force size | 4 million (number = strength) | unchanged | Reduced to 3 million (for better integration) | Reduced to 2.5 million | Presumably even smaller |

| Main objective | Homeland defense | Defend China closer to its borders and fight mobile style of war | Win local wars on China’s periphery | Deter Taiwan from independence; deter US from intervention | Employ IW by bypassing all the deficiencies (electromagnetic dominance) |

| Main threat | USSR | USSR | Regional skirmishes | Taiwan US | US |

| Main limitation | Budgetary constraint | Budgetary constraint | Budgetary constraint | Doctrine-capability gap | Technology |

| Main catalyst | Modernization in the aftermath of the Cultural Revolution | Changing threat perception | Changing security posture | The Persian Gulf War and the end of the Cold War | Information revolution |

| 1978-85 | PD | PL |
| 1985-88 | RD | PD | PL |
| 1988-92 | RD | PD | PL | PPL |
| 1992- | RD | PD | PL |

**Legend:**
- PW: People’s War
- PWUMC: People’s War under Modern Conditions
- LW: Local War
- LWUMHTC: Local War under Modern High-Technology Conditions
- RMA: Revolution in Military Affairs
- PD: Primary doctrine
- PL: Preliminary doctrine
- PPL: Pre-preliminary doctrine
- RD: Residual doctrine

People’s War

In the late 1970s, the PLA, over four million strong, was structured, using the doctrine of “people’s war,” to defend the Chinese mainland from threats such as the Soviet Union. Emerging from the turbulent Cultural Revolution (1966-76), China’s reformist leaders acknowledged the need for military modernization, but nonetheless assigned it last among the Four Modernizations. The low priority for military modernization translated directly to low defense budgets, a situation that was a key constraint on military modernization into the late 1990s.

The PLA’s force structure was dominated by the army and had a continental orientation. Its ground forces were organized around infantry corps, also called field armies, which generally had three infantry divisions and smaller armor, engineer, artillery, and other combat support or combat service support units. A large militia would complement main and local force units as they “lured the enemy in deep.” Air and naval forces primarily had a defensive mission and, for the most part, operated independently of the ground forces.

People’s War under Modern Conditions

In the late 1970s and early 1980s, PLA strategists began considering a doctrinal revision that was intended to defend China closer to its borders and fight the Soviets in a more mobile style of war with a combined arms and joint force. The use of nuclear weapons also was envisaged. The new doctrine became known as People’s War under Modern Conditions.

It called for a more flexible, professional PLA, incorporating increased numbers of modern weapons into its inventory. The ground forces emphasis shifted more to tanks, self-propelled artillery, and armored personnel carriers. However, the cost of equipping enough of the force with sufficient modern
weapons to fight the Soviets was prohibitive to the Chinese budget. Beginning in the 1980s, PLA infantry units began to be issued enough trucks to make them road-mobile.

Local War

Between 1985 and 1988, PLA personnel were reduced to three million. The reduction would permit the integration of branches of the PLA ground forces with its naval and air forces, a requirement to conduct modern warfare. In 1985, Deng Xiaoping forecast that the threat of a major war was remote. Instead, the more likely scenario would be a limited, local war on China’s periphery. The formation of small, mobile, “Fist” or “Rapid Reaction Units (RRUs) was a major organizational development peculiar to the Local War doctrine. Despite these dramatic changes in the military, however, defense budgets remained tight until the end of the 1980s.

The PLA suffered a blow to its prestige as a result of its role in the 1989 Tiananmen massacre. One method to boost its prestige was to increase its budget and purchase new weapons. Meanwhile, the demise of the Soviet Union provided an opportunity to the Chinese government to spend some of the new money it now was willing to devote to the military for the purchase of advanced military hardware that the West had denied to China since 1989. The implosion of the USSR also forced the PLA to reexamine the threat it faced.

Local War under Modern High-Technology Conditions

The Gulf War forced a change in the attitudes of many of the PLA old guard, who emphasized the role of man over weapons. The war was said to be an example of what the PLA theoreticians now called Local War under Modern High-Tech-
nology Conditions (LWUMHTC). By the mid-1990s, LWUMHTC had become the dominant doctrine in the PLA. At the same time, some PLA strategists expanded their study of other concepts of future high-technology warfare, including IW, which became known under the rubric, RMA. Between 1997 and 2000, another half million personnel were shed from the ranks. The major focus of PLA operational planning in the late 1990s had become the preparation of military options and capabilities to ensure that Taiwan would not seek independence. The possibility that the US military might become involved in the defense of Taiwan is a worst-case factor that PLA planners also must consider. Taiwan's location invites scenarios of LWUMHTC to be applied to it.

It should be pointed out that, for the past two decades, multiple doctrinal concepts have existed or been in development concurrently within the PLA. Even though the size of the PLA and its doctrine have changed over time, elements within it differ in structure, mission, and doctrinal orientations, yet exist concurrently. Even today, many ground force units still are best suited for People's War operations to defend the Chinese mainland. Others, such as the RRU s, have mobilized to the point that they are trained for a role in LWUMHTC. A very few units, such as missile and electronic warfare units, also are beginning to develop capabilities suitable for twenty-first century RMA warfare, in addition to being integral to Local War scenarios.

IW holds special appeal to top PLA brass, which sees it as a way of bypassing all the deficiencies most PLA commanders and researchers recognize. Sometimes these are referred to as “killer” weapons or “trump cards” or “magic weapons” (shashoujian) that can overcome inherent weaknesses in the PLA to inflict surprise attacks.32

Noting these interesting (and some even farfetched) discussions, Paul Godwin, a respected American expert on the PLA, provides a more realistic assessment. He asserts that a persistent "doctrine-capability gap" exists—in other words, doctrinal development seems often to have gotten ahead of actual force modernization.

Simply stated, the vast majority of China’s ships and aircraft are obsolete. . . . 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.\(^{33}\)

That the Chinese are nevertheless serious about IW indicates that they anchor their IW strategies in a broader politico-military context and seek to compensate technical inferiority with good strategies. Their approach marks an interesting contrast with the mainstream Western concepts of IW.

**Elements of China’s IW Strategies**

In theory, information and asymmetric warfare can alter traditional power structures because a weaker state can plausibly penetrate its stronger enemy’s network system. However, 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 into a network-based organization, integrating the military system so that it can interlink and interact to create a limitless extension of its arms and services. Joint operations, network warfare, and information warfare have enabled one another’s mutual growth, providing both tremendous strengths and weaknesses for the military capabilities of

---

\(^{33}\) Godwin, “Compensating for Deficiencies,” 114.
stronger states. Networked IW represents an intriguing progress: moves toward information systems and networks not only are advantageous but increasingly necessary for stronger states.

However, while network-based operations enable enhanced coordination of skilled attacks, a dependence on information can leave the military vulnerable to attacks on its information base, leaving its divisions disintegrated and helpless. Thus, the side of strong American information knowledge also potentially exposes a weak side to a determined and increasingly sophisticated adversary.

China's IW Possibilities

The Chinese thinkers are keen on these paradoxes. For example, PLA scholar Su Enze notes that the irony of IW is, as states develop further technology, it is easier to reproduce and also becomes more vulnerable to attack.

As technology and know-how continue to spread throughout the world, American resource advantages in regard to the security of its information and information systems gradually may erode vis-à-vis a weaker but determined rival that is developing IW capability before more resources and technological developments are initiated to reestablish the lead. PLA strategists reason that the field for offense-defense calculation appears temporarily leveled during such "windows of opportunity." A recent PLA publication postulates that advantage goes to a 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.

However, the author also emphasizes the importance of defensive IW:

Owing to the fact the material resources the offensive side needs in an information warfare are relatively little, and the most precious resources are the attacker’s wisdom and resourcefulness, the traditional strategy of “defending by attacking” – a concept based on the conservation of total resources – is no longer useful; whereas “making all-out attack and all-out defense” and “balancing attack and defense” should be the proper guiding thought for the studies of modern information warfare.36

This recent article reflects a gradual maturation of China’s IW discourse, moving from a focus on offensive IW’s asymmetric advantages that favor the weaker party, a view predominant in earlier scholarship, to a more clear-headed reevaluation of China’s underdeveloped IW defense (vis-à-vis a technologically advanced rival). However, some concepts of earlier scholarship are interesting in that they focus on gaps (theorized or real) in America’s information systems.

For example, through an information attack, the PRC seeks to successfully utilize the principles of asymmetric warfare by crippling a stronger military (US) through the isolation and penetration of a gap in its network. Chinese IW usually focuses on a singular “zone” of weakness, and is able to overcome its traditionally inferior force by exploiting the weakness of the stronger military. The goal of American joint operations, or the networking of its military around information systems, is the comprehensive integration of units for all military purposes. By contrast, the goal of Chinese joint operations, as

---

36 Both quotes are from Tang, “Information Security.”
indicated by Chinese military journals, is the concentration of its "capabilities" in a certain direction, or zone, with the intention of creating superiority over the enemy, in a specific area, at a specific time.

Thus, the Chinese concentrate on exploiting weaknesses in stronger states rather than on developing their own comprehensive strength. Their 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" (qunlong wushou). This illustrates a fundamental attitudinal change in military thought: rather than competing with strong states, weak states are well served to explore asymmetric warfare.

Besides network destruction, endless possibilities exist for the development and execution of Chinese asymmetric warfare. The attainment of long-range precision interception weapons, the use of unused frequencies in civilian T.V. and radio broadcasting for information communication, encryption-based codes to prevent information stealing, space and satellites to obtain intelligence, use of saturated tactical ballistic missiles, and the development of a directional infrared jamming system all are among Chinese possibilities.

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. Submarines play a large role in the Chinese asymmetric plan, as well as space warfare that can be conducted by ships to destroy the enemy's satellite information. In 1996, the People's Liberation Army Daily recommended

---

that China develop its own "unique lethal weapons" rather than try to replicate old frameworks with new technologies. It also suggested that a macro-control system be established to exploit developed countries that depend on networks and consequently are "fragile and vulnerable."  

The asymmetric use of such weapons and techniques evinces the changing notions of traditional, attrition-based power. A superior navy could be defeated through the disabling of its space-based communications, the utilization of shore-based missiles, or "magic weapons," such as tactical laser weapons. Targets of asymmetric attack could be electrical power grids, civilian aviation systems, transportation networks, seaports and shipping, highways, and television broadcast systems.  

From a larger strategic standpoint, asymmetric warfare holds further appeal to Chinese leaders. Since 1978, Chinese leaders have pursued a fundamental national strategy that seeks to elevate China's overall national power by focusing on economic development. The PLA thinkers mentioned earlier argue that IW may allow their country to compete with the United States militarily, without sacrificing resources designated for economic growth.

Overcoming the Superior with the Inferior

At a COSTIND (Commission of Science, Technology, and Industry for National Defense) National Directors conference on December 22, 1995, Liu Huaqing, China's top admiral, declared:

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 revolu-

---

39 Ibid.
tion with information warfare as the core has reached the stage where efforts must be made to catch up and overtake rivals (emphasis added).\textsuperscript{40}

The PLA reckons that, throughout its history, it has had to overcome several stronger rivals: the KMT (the Chinese Civil War), the US (the Korean War), and the USSR (the Sino-Soviet border war). So the concept of “overcoming the superior with the inferior” is deeply ingrained in the PLA’s ethos and mythology. Whereas in the past the PLA had been able to compensate for its firepower or manpower with superb unconventional or nonmilitary strategies, such as guerrilla warfare, psychological warfare, political propaganda, and united fronts, the PLA now feels strongly that in the twenty-first century it must harness high technology in its struggle against its most probable and powerful strategic rival, the US. In developing IW, the Chinese still believe that superior strategies can help overcome technological deficiencies.

The Chinese thinking is consistent with a recurring puzzle: why would a weaker party take on a stronger party, rather than accept an objectionable status quo, as Mor puts it? Asymmetric conflict challenges classic deterrence theory, which posits that the status quo deters anti-status quo power due to the former’s preponderant capability.

\textit{Asymmetric Conflict: An Enduring Allure}

The concept of the weak overcoming the strong is not a concept unrecognized by Western scholars. For example, Thazha V. Paul’s study compared six cases of war initiated by the weaker powers and studied the dynamics of asymmetric conflicts.\textsuperscript{41}

In an interesting article published in 2001, Ivan Arreguin-Toft examines under what conditions the weaker powers actu-

\textsuperscript{40} Quoted in Mulvenon, “The PLA and Information Warfare,” 179.
\textsuperscript{41} Paul, \textit{Asymmetric Conflicts}.
ally win the war.\textsuperscript{42} His study shows that, among all the asymmetric conflicts in the 1800-1998 period, the strong actors won 70.8 percent of the time, whereas the weaker party won the other 29.2 percent. However, his more interesting findings show that, over time, the weaker actors won an increasing percentage of asymmetric conflicts. By breaking the period under study into four fifty-year segments, he finds that 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 1800-49, and 20.5 percent for 1850-99.

However, the weaker actors fared much better as examined by the evidence from the twentieth century. They won 34.9 percent of all asymmetric conflicts for 1900-49, and 55 percent for 1950-98. That is, in the latter half of the twentieth century, not only were the weaker actors more prone to initiating conflicts than in previous periods, but also they were more likely to win (with the Vietnam War being a prime example)! These findings challenge traditional concepts of IR and should be of considerable interest to countries like China.

Arrenguin-Toft proceeds to analyze the various scenarios under which strong states can be defeated by their weaker counterparts. He refers to the thinking of Mao Zedong that, when the weak fight the strong, the weak will benefit from certain interaction of direct and indirect approach strategies. He defines direct approaches as aiming to dismantle an adversary's \textit{ability} to fight, whereas indirect approaches aim to destroy the adversary's \textit{resolve} to fight. He postulates that, when strong actors attack with a direct strategy and weak actors defend 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 also will win. In short, when the stronger and the weaker actors' approaches converge, the stronger actor is

\textsuperscript{42} Arreguin-Toft, "How the Weak Win Wars."
expected to win, but when their approaches diverge, the weaker actor is expected to win.

In both cases, the weak actor will win because, in both cases, the intersection of strategies will prove time-consuming for the stronger actor, while the weaker actor will remain resilient. Underlying this idea is the concept of "interest asymmetry," whereby a strong state will be subject to the notion of "relative interest"; because its survival 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 withdrawal of the strong state's presence in a situation where it is suffering significant losses, even though that state may have the superior military resources.

Arenguin-Toft sums up the expected effects of strategic approaches on conflict outcomes in a 2x2 matrix, with the expected winners identified in the cells.

### Weak-Actor Strategic Approach

<table>
<thead>
<tr>
<th></th>
<th>Direct</th>
<th>Indirect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strong-Actor</td>
<td>Strong actor</td>
<td>Weak actor</td>
</tr>
<tr>
<td>Strategic Approach</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indirect</td>
<td>Weak actor</td>
<td>Strong actor</td>
</tr>
</tbody>
</table>

### The Gulf War Wake-up Call

The effective use of American IW during the Gulf War caused certain countries to examine their use of information weaponry. The PLA took notice not only of American supe-
rior technology, but also of the destructive power of US joint operations, created through the "synergy" of multiservice actions. US joint operations included simultaneous attacks from Air Force and Navy aircraft, Army attack helicopters, and Navy strike missiles. Such operations blinded, deafened, and quickly destroyed opposing forces. The PLA realized that both its "people's war" ground troops and its military doctrine were rendered obsolete.

The PLA examined American military techniques, and determined that it would focus on strategic, operational, and tactical reconnaissance. Meager resources granted for military modernization focused on joint operations as influenced by American use during the Gulf War; air and naval forces received funding because General Liu Huaqing realized land and sea battles could not be won without integrative support.43 Thus, the Gulf War served as a catalyst for the PLA's development of information warfare, and also served as a marked change in traditional power structures.

IW to Spearhead Military Modernization?

As stated before, military modernization, designated as the last of the Four Modernizations, received modest attention from the late 1970s to the early 1990s, largely due to budgetary limitations. However, the demise of the Soviet Union, the end of the Cold War, and China's double-digit growth in the 1990s have allowed China to substantially increase its military spending and to use its new-found wealth to acquire advanced weapons and technologies.44

---

44 Ascertaining the true figures of China's defense expenditure is a matter of considerable debate. In March 2002, Chinese finance minister Xiang Huaicheng announced that China is increasing military spending in 2002 by 17.6 percent, or $3 billion, bringing the publicly reported total to $20 billion. However, the publicly disclosed figures do not include major spending for weapons research and foreign arms purchases. The Pentagon report estimates
Since China’s defense industrial complex lags in developing high-technology equipment, China must find “selective pockets of excellence,” according to the late Chinese leader, Deng Xiaoping.\(^{45}\) IW plays a very important role in this strategic view of military modernization.

As an example, China now arms its vast 1.5 million-strong reserve force, whose main role in the past had been to support PLA forces in defense against foreign intervention, with IW/IO (information operations) missions. In response to Chairman Jiang Zemin’s 1991 call for building common telecom systems for military and civilian use, China’s reserve telecom regiments have become the high-tech link in the country’s “people’s war” theory.\(^{46}\) Ideas for uniting a people’s war with IW are finding fertile ground in China’s reserve force. Several IW reserve forces already have been formed in Datong, Xiamen, Shanghai, Echeng, and Xian. Each is developing its own specialty as well. For instance, Shanghai reserve forces focus on wireless telecom networks and double-encryption passwords.

**Chinese vs. Western Concepts of IW**

Assessing the implications of China’s IW strategies requires an understanding of the distinct ways the Chinese and Americans approach the concepts, definitions, and limitations of information warfare. Cultural bias, traditions, and present

---


attitudes regarding warfare strategy prevent a uniform interpretation of IW. Thus, Western and Chinese understandings of information as a mechanism of war may vary greatly.

Among Western scholars, there is a consensus that information warfare is a series of combat actions taken to attack the enemy’s systems of information, while preserving one’s own information and information systems. However, a traditional Soviet/Asian interpretation of information warfare is more encompassing, including the offensive and defensive nature of peacetime, crisis, and war operations, as well as national, strategic, and tactical levels of operations during times of war.

Traditionally, Western military scholars have been concerned with offensive information warfare as it relates to the enemy’s command and control center, whereas Eastern military scholars include the elements of electronic, psychological, virtual, and economic warfare, and even CNN coverage and the destabilization of financial institutions. By contrast, the Chinese/Soviet definition of military science involves not only military operational art, but also specific approaches broadly included in military art, such as psychological trickery, stratagems, etc. There is no American counterpart to this idea of military science. Chinese strategists study the changes in war as a scientific forecast, whereas American military scholars focus on the “almost accidental” role of military genius that changes concepts, allocations, and technologies.

Emerging differences in Western and Chinese interpretations of information warfare are significant because they challenge the conventional wisdom of power politics. Western theorists view information as a weapon to be used on a limited scope and as a mechanism to preserve more conservative structures. Eastern military theorists interpret information warfare as an equalizer through the use of asymmetric and

---

broad-reaching techniques. Thus, discrepancies in the military philosophies have profound implications on international power politics.

Challenges to Western Mainstream Concepts

Although American success in the Gulf War awed the PLA with the execution of technology and joint operations, causing it to reexamine its military technologies and strategies, the Chinese seem aware of the peril of duplicating American IW. Instead, they seem more interested in developing “information warfare with Chinese characteristics.”

Chinese authors’ writing on information warfare borrowed the Western idea of information dominance, but their methods for achieving information dominance differ from those of the West. Information warfare creates ambiguities and uncertainties, complicating the tasks for military planners to prepare for contingencies. In information warfare, superior strategies are as important as advanced technologies. The Chinese see the application of certain ancient stratagems as a way to possess a superior ability to execute strategy and to develop a complementary military doctrine for modernizing their forces.

Interestingly, Chinese IW strategies revitalize the execution of the classic Thirty-Six Strategies: The Secret Art of War.49 There are clear IW connections to the first five strategies, in which information creates an environment of anonymity, ambiguity, and the confusion and dilemma of ethical retaliation that Chinese long have dominated traditionally.50

If one fails to consider that America’s comprehensive strength actually can become a weakness, as previously argued, then it may seem impossible that such isolated “pockets of excellence” and strategizing even could dent a super-

50 Thomas, “China’s Electronic Strategies.”
power such as the United States. Thus, it is plausible that, 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 still can betray weaknesses and China’s comprehensive weakness may become its strength – the type of paradox Chinese military officials have recognized and exploited for centuries.

As demonstrated by the Gulf War, the United States was the leader in the use of information warfare and the exploitation of joint operations. The PRC has followed US doctrines on information warfare as they relate to technologies and joint operations strategies. However, this emulation by the PRC should not suggest that the PLA is any less of a potential threat to American security. As information weapons and technologies lead to joint operations, such network-based information systems become highly vulnerable to the rise of asymmetric attack. While the strength of the US lies in technological and strategic mechanisms for information, the mechanisms' movements leave significant network gaps open for asymmetric attack, granting the PRC the exercise of its strong suit – asymmetric tactics.

The PRC's history boasts a legacy of the weak defeating the strong. So while it is true that the US may lead the PRC in information technologies and techniques, the PRC's potential threat cannot be dismissed both because its military history encompasses the techniques of asymmetric warfare and because its interpretation of warfare is far more encompassing than a traditional Western view. This allows for a far greater scope of destruction – entering private, civilian spheres.
Seeing Chinese IW in Action

Despite the assiduous scholarly interest concerning IW, the PRC's IW capability is hitherto far from operational (or "weaponized"). This section provides early glimpses into the various ways China has conducted early examples of IW as a way to speculate how future conflicts may look. Applying IW has presented technical ironies to the PRC: the presumed assurance of information domination and advantage of asymmetry does not work entirely in the PRC's favor; and the PRC is not immune from the same vulnerabilities that its IW warriors seek to exploit in the adversary. This section focuses on 1) cybernationalism, and 2) IW combined with amphibious assault.

Cybernationalism: When Nationalism Meets the Internet

Scholars have discussed the reasons for the rising nationalism in China in recent years – government manipulation, public confidence and pride as a result of economic development, and anti-American sentiment – and speculated about the implications of this nationalism on regional security and US policy.\(^{51}\)

This rising nationalism coincided with an explosive growth in China's Internet population. The best industry publication estimates that, in barely three years from 1997 to 2000, China's online population had increased from 200,000 to 16.9 million, making China one of the largest and fastest-growing markets.\(^{52}\)

---


52 By another measure – Internet “penetration rate” (online population as a percentage of total population – China remains sparsely wired. For the same
The advent of information technology and its popularization curiously have lent a "weapon of choice" to Chinese nationalism. Chinese chat rooms now are filled with strident nationalistic messages. Most of these outbursts can be dismissed as harmless, irresponsible "freedom of expression," and they seem to enjoy the tacit permission of the authorities, who view protests in cyberspace as a preferable alternative to protests in the streets. However, occasionally when China has been amid a foreign policy flap with an outside actor (the US, Japan, or Taiwan), these disparate expressions have coalesced or been mobilized to promote the PRC’s interests and viewpoints – a phenomenon this article shall call "cybernationalism." Two cases are in point.

According to a Taiwanese report based on intelligence sources, after former Taiwan President Lee Teng-hui enunciated his view in July 1999 that, henceforth, relations between Taiwan and the mainland should be "special state-to-state relations," hundreds of Chinese hackers attacked or attempted to invade Taiwanese Web servers. Retaliation from Taiwanese hackers resulted in the destruction of many Web sites and computers on both sides. The 1999 "cyberwar" actually exposed the vulnerability of computer systems on both sides. The same report quoted China’s PLA Daily, which advocated the need to cultivate high-quality "Internet warriors" who could be trained by select universities in China and combined with computer experts from the private sector.

Chinese cybernationalism reached a zenith in May 2001, as a result of a series of tensions in US-PRC relations: the April 1 collision of military planes, President Bush’s statement that the US would do “whatever it takes” to help Taiwan

period (1997-2000), China’s Internet users rose from 0.001 percent of the total population to 1.34 percent. NUA Internet Surveys, “NUA Internet How Many Online: Asia,” 2001, available at <http://www.nua.ie/surveys/how_many_online/asia.html>.

defend itself from Chinese attack, and the sale to Taiwan of a robust package of defensive arms. A self-styled Honker's Union, a network of Chinese nationalistic hackers, took up China's nationalist cause. The group's name in Chinese means "Red hackers," indicating the political motives for their actions. Honkers maintained that they differed from other hackers because they did not act out of malice. They utilized modern IT (their Web site, e-mail system, and downloadable viruses) to recruit fellow patriots in a "people's war" against the US by attacking thousands of American Web sites. They announced in advance that their attacks would coincide with politically sensitive dates, such as May 1 (International Workers' Day) and May 18 (the second anniversary of the NATO bombing of the Chinese embassy in Belgrade). They succeeded in defacing one thousand US Web sites with pro-China messages, paralyzing an untold number of computer systems, penetrating the public information page of the White House, and destroying all data on Web servers to which they were able to gain access. But their attacks also triggered a furious retaliation by hackers based in the US, who indiscriminately attacked all sites with the domain name "cn," resulting in the destruction of hundreds of Chinese Web sites.

What is the practical impact of this early showing of possible IW? One can view the above case of "cyberwar" as a virtual substitute to an actual armed conflict between the US and the PRC, in which there is no casualty. However, this case actually reveals an incipient "mutual assured destruction" (MAD) of some sort in the application of IW. The Chinese boast of IW's offensive advantage was humbled by the vulnerability of its own information systems from the adversary's


attack. Other than leaving the nuisance of having to clean up these electronic equivalents of graffiti, China’s IW has not fundamentally changed its balance of power vis-à-vis the US nor advanced its goal of absorbing Taiwan. "Digital MAD" dampened early Chinese euphoria over IW.

IW in a Taiwan Strait Contingency

A second case of IW application entails more significant security implications. PLA officers have promoted IW as an effective weapon to subdue Taiwan and deter possible American intervention.56 Here, the PLA seeks to gain information domination in a conflict with Taiwan by attacking Taiwan’s command and control centers and information networks, and by conducting propaganda and political warfare. The purpose is to incorporate Taiwan into the PRC by "subduing the enemy without actually fighting," à la Sun Tzu, and by denying possible American military intervention.

The recent Pentagon report points out that, although China’s communist leaders have professed their rhetorical commitment to a peaceful unification with Taiwan (on Beijing’s terms), certain trends, such as official statements lengthening the list of conditions under which Beijing would use force against Taiwan and the PRC’s ambitious military modernization program, may reflect an increasing willingness to consider the use of force to achieve unification. The report states that “Beijing’s primary political objective in any Taiwan-related crisis, however, 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.”

The Pentagon report concurs with the view of certain analysts that the PLA’s offensive capabilities improve as each year passes, providing Beijing with an increasing number of credible options to intimidate or actually attack Taiwan.

In addition to other weapons slated for asymmetric warfare, such as ballistic missiles, the PLA views IW as a credible military option for achieving Beijing’s political objectives and has made considerable efforts toward making IW a real alternative.

The PLA conducted large-scale war games in the Taiwan Strait in summer 2001. For the first time, the exercises began 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. In its exercises in 2002, the PLA incorporated more sophisticated items of IO/IW.

This scenario presents a new challenge to US strategic planners. Most analysts hitherto have:

- Dismissed the Chinese invasion threat due to the high threshold for success (logistical difficulties, Taiwanese resistance, and international intervention),
- Argued that Taiwan’s smaller military can maintain a qualitative edge until at least 2005,
- Questioned whether Beijing has realistic military options vis-à-vis Taiwan, despite its consistent refusal to renounce the use of force and its occasional saber-rattling against Taiwan, and
- Believed that a probable, albeit not guaranteed, US military intervention (in the case of unprovoked attack on


Taiwan) serves to deter Beijing (the policy of so-called strategic ambiguity).

However, many Chinese strategists now believe that IW has lowered the threshold for a successful military campaign against Taiwan and has increased the utility of an offensive strategy, because it holds promise for “winning the battle without fighting” (Sun Tzu’s adage) and “overcoming the superior with the inferior” (Mao’s guerrilla strategy). Properly executed (with deception, surprise, precision, and decisiveness) along with other coercive weapons (e.g., missile strikes and a naval blockade), IW may help bring Taiwan to its knees and deny American intervention.

Paradoxically, both technology and misperception may cause China to be more, rather than less, likely to use force, regardless of the words or deeds of Taiwan’s leaders. So the application of information technology in international conflicts, such as cross-Strait tensions, may have a negative impact.

However, the perceived advantage to offense in IW will last only if the adversary fails to take proper countermeasures to augment its offensive and defensive IW capabilities. To counter China’s IW development, Taiwan has made its own endeavors in IW. In summer 2001, Taiwan’s military established its own electronic-warfare unit.60 In June 2002, Taiwan for the first time incorporated a drill in its decades-old Wan-An air-raid drill to boost the island’s Internet defenses against hacker attacks, especially from China.61 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.

• To prevent war by building a sustainable defense capability so that "the enemy dare not rashly wage a war,"
• To maintain stability in the Taiwan Strait through dialogue and exchange on security issues between the two sides, and
• In the event of an invasion, to be ready to defend itself.62

The Taiwanese white paper notes China’s expanding military power, including its efforts to acquire capabilities, such as space, electronic, information, and precision attack warfare, which would enable it to conduct first strikes in wars against Taiwan. In response, it calls for Taiwan to build a “compact but delicate, highly capable” modern force by reducing the number but 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; and maintaining air superiority and naval dominance.

Until a “digital MAD” of some sort is established in the Taiwan Strait, the PRC’s IW development has introduced uncertainties and risks in this volatile region. This is a case of how technology, combined with intentions and (mis)perceptions, may become a destabilizing factor for international security.

Conclusion

This article has explained the perceived strategic utility of IW to the PRC and reviewed the PLA’s discourse and early applications of IW. The remaining space is devoted to a brief discussion of some of the implications of asymmetric warfare.

Rather than giving definitive answers, the discussion is intended to raise questions for further research.

First of all, interstate conflicts have not ended. Instead, as illustrated in the case of IW, they now are driven increasingly by new technological factors and have taken on new forms, particularly the multiplication of actors (state and nonstate, both engaging in interstate conflict).

This raises the issue of technical irony. The irony stems from the double-edged nature of information technology. On the one hand, today a nation's economic prosperity and military strength rely on technological supremacy. On the other hand, the dependence of postindustrial societies on the Internet and computer networks also gives the weaker parties (states or terrorists) opportunities to exploit this vulnerability. Information warfare has the allure of an asymmetric war.

There is a further irony: although information technology entails beneficial potentials (narrowing the wealth gaps by empowering the poor, both within and across countries, or contributing to peace by virtue of deterrence), it can cause misperceptions and miscalculations on the part of the weaker offensive party that overestimates the utility of offense and underestimates the cost of defense.

In the case of the PRC, IW may tempt PLA commanders to move away from active defense toward a preemptive strike. China's design for Taiwan most likely is a short, decisive blow that results in Taipei's capitulation, i.e., a fait accompli presented to the international community, rather than a protracted campaign, such as amphibious invasion or embargo, that has to deal with uncertain consequences from other actors.

IW appears especially attractive in this regard, because it promises a quick resolution of the military contingency and low casualty in order to preserve Taiwan's industrial and commercial assets for Beijing.

As stated before, Taiwan has responded with its own IW endeavors. Whether Taipei's strategy aims to protect its own
information resources or to mimic Beijing’s “asymmetric warfare” strategy by targeting Beijing’s vulnerable areas, will have implications for whether this development will contribute to stability by virtue of the threat of a digital MAD, or to more instability by introducing a spiraling security dilemma.

Second, how seriously should American defense planners take the PRC’s endeavor in IW? That the PLA is immersing itself in concepts of RMA and that Beijing’s acknowledgement of a doctrine-capability gap perversely may convince it to commit more resources to the development of the weapons and equipment called for by its IW doctrine, are of natural concern to Pentagon planners who have the responsibility for maintaining peace and stability in the Western Pacific.

Although it is true that, at the present time, modernization of the Chinese force has lagged behind doctrinal development, China’s recent history (e.g., indigenous development of atomic bombs in 1964 and alleged indigenous development of the warhead miniaturization technology) suggests that development of an “IW with Chinese characteristics” is not entirely far-fetched. Americans ignore, at their own peril, that the synergy that results from technology and strategy in the information age can take more than one (US) form.

This article has not given definitive answers to the problems of information warfare, but it encourages further research that can help us to “seek truth” more aggressively on this important emergent issue.