AIR WAR COLLEGE
AIR UNIVERSITY

China as Peer Competitor?

Trends in Nuclear Weapons, Space, and Information Warfare

KATHRYN L. GAUTHIER
Lieutenant Colonel, USAF

Air War College
Maxwell Paper No. 18

MAXWELL AIR FORCE BASE, ALABAMA

July 1999

Disclaimer

Opinions, conclusions, and recommendations expressed or implied within are solely those of the author and do not necessarily represent the views of Air University, the United States Air Force, the Department of Defense, or any other US government agency. Cleared for public release: distribution unlimited.

Foreword

In *China as Peer Competitor? Trends in Nuclear Weapons, Space, and Information Warfare* Lt Col Kathryn L. Gauthier analyzes the potential for China to emerge as a peer competitor of the United States in the coming decades. First, she examines two traditional pillars of national strength—China's status as a nuclear weapons state and as a space power. Second, she then explores China's growing focus on information warfare (IW) as a means to wage asymmetric warfare against a technologically advanced adversary. Third, the author carefully examines the status of the three programs, highlights areas of concern and potential conflict with the United States, and analyzes the implications of these issues for the United States.

The author concludes that China does have the potential to become a peer competitor, based on a number of factors. The United States's military advantages over China are narrowing in the critical areas of nuclear weapons, space technology, and information warfare. China is developing nuclear weapons with increased accuracy, mobility, and range. Beijing's growing prowess in space—including a possible manned presence within the decade—will also provide it significant benefits in the military realm. In selected areas, Beijing has demonstrated its ability to "leapfrog" over more rudimentary stages of technological development. Finally, China's previously rapid economic growth has supported technological modernization and an improved defense posture.

Colonel Gauthier emphasizes that Beijing does not—either philosophically or militarily—have to approach US levels of capability or proficiency to pose a threat to the United States or to US interests in the region. There is clear evidence the Chinese are vigorously analyzing, pursuing, and acquiring the means to wage asymmetric warfare against a more powerful adversary. Asymmetric warfare can be cheap, low tech, readily available, and devastatingly effective against the United States. For these reasons, information warfare may prove to be the "weapon of choice" for the Chinese; given the vulnerability of the US infrastructure and China's more rudimentary military information systems, China could actually hold the "high ground"

in this arena in the future. In keeping with its long-stand ing cultural and strategic traditions, Beijing would likely attempt to "defeat the enemy without fighting" by playing its information deterrence card. Alternatively, it could at tempt to carry out a surprise IW attack with sufficient deception to avoid retaliation.

The author does not believe it is inevitable that China will become an adversary of the United States. But this possibility could become a self-fulfilling prophecy if the United States mishandles its relationship with China. Colonel Gauthier advocates a policy of constructive en gagement with the People's Republic of China, believing the United States holds some of the cards with which to positively shape the future of Sino-US relations, and the specter of a militarily capable and potentially hostile China makes a compelling case for doing so. The Air War College encourages a debate of these views.

Major General, USAF
Commandant
Air War College

About the Author

Lt Col Kathryn L. Gauthier is assigned to the J5 directorate of the Joint Staff. Her 18-year Air Force career includes recent tours as chief of inspections for the Air Intelligence Agency Inspector General team and commander of the 426th Intelligence Squadron. She has also served as a joint intelligence center branch chief, political-economic analyst, telemetry systems development engineer, and airborne mission coordinator, with duty stations in Latin America, Asia, Europe, and the United States. While an Olmsted Scholar, Colonel Gauthier earned master's degrees in political science and international public policy through advanced studies in Caracas, Venezuela, and Washington, D. C. She is a graduate of the Spanish Air Staff College in Madrid, Spain, and the Air War College, Maxwell Air Force Base, Alabama.

China's Nuclear Program

> By the early 21st century, the PLA's nuclear arsenal will be more capable, accurate, flexible, and will allow the PRC to threaten most parts of the globe. Land-based missile systems will be mobile, enhancing survivability and making detection much more difficult. Sea-based systems, with longer ranges, will also be tremendously improved.
>
> —John Caldwell and Alexander T. Lennon
> "China's Nuclear Modernization Program"
> Strategic Review 23, no. 4 (Fall 1995)

What threat will the People's Republic of China (PRC) pose to the United States? To some, it is an expansionist power set on regaining the hegemony it enjoyed centuries ago in Asia. Beijing's aggressive moves toward Taiwan and its moves in the South China Sea are used as evidence of such poorly concealed ambitions. Some further claim the PRC is set on achieving global power status. This raises the specter of an awakened China set on redrawing the maps, restoring the splendor, and recreating the power of the "Middle Kingdom" before it fell to the advances of Western imperialism.

Others argue that today's China has a quite distinct worldview. They see an inwardly focused, nonaggressive, developing nation. This China is so burdened with internal problems arising from the necessity to provide basic services for a quarter of the planet's population that it has neither the time nor the inclination to harbor hegemonic aspirations in the foreseeable future. Further, any change in that status is likely to take decades, allowing for ample strategic warning time and the opportunity to respond appropriately when the time comes.

This paper sets out to analyze the threat, if any, that China poses to the United States as the world's sole remaining superpower. Specifically, it seeks to answer the question, "Does China have the potential to become a peer competitor of the United States in the coming decades?" A search for the answer to that question requires an exhaustive analysis of not only military and industrial potential but also the economic, social, and political trends that are sweeping the nation. Even then, since the issue involves

both capability and intent, the conclusion might be predic-tive but never definitive.

Given both the complexities of the issue and the time constraints, this paper focuses on three strategic factors in the peer-competitor equation. It examines two traditional pillars of national power—China's status as a nuclear weapons state and as a nation in space. Then it explores China's increasing focus on information warfare as a means of waging asymmetric war against a more powerful adversary. Why the selection of these three factors?

One of the lessons of the Gulf War was the inability of a strong adversary to defeat a technologically superior foe with conventional weapons and war-fighting techniques alone. An enemy facing the United States with a nuclear arsenal—or even one bomb—however, quickly changes the equation. So does one with self-sustaining access to space or one armed with antisatellite weapons. Finally, an adver-sary unwilling to confront the United States "head on" might still seek to achieve strategic objectives through such asymmetric means as attacking the information sys-tems of the United States, a nation highly dependent on access to information in both peacetime and conflict. In sum, since these three elements—nuclear weapons, access to space, and capabilities in the information-warfare arena—could arguably pose the greatest threat to the United States in a future military conflict with China, they were considered a foundation for China's potential emer-gence as a peer competitor to the United States.

China's Nuclear Arsenal

China became a nuclear weapons state in 1964 and since that time has conducted 45 nuclear weapon tests with yields ranging between approximately 1 kiloton and 4 megatons.[1]

Characteristics

While China has never disclosed the size and disposition of its nuclear force, analysts estimate the entire arsenal consists of perhaps 250 to three hundred strategic war-

heads and 150 tactical warheads.[2] Beijing has never ac-knowledged the existence of any tactical nuclear weapons in its inventory.[3] The US Defense Department believes China has more than one hundred warheads currently de-ployed on ballistic missiles.[4] China is also estimated to have a stockpile of fissile material sufficient to double or triple the size of its current nuclear arsenal.[5]

Doctrine

Although it is ranked as the world's third largest nuclear power,[6] China has a nuclear inventory that is small relative to those of the United States and Russia. Beijing maintains that its small nuclear arsenal is for self-defense purposes only.[7] China has always maintained a policy of No First Use (NFU) and has long provided negative security assur-ances (NSA) that it would never "use or threaten to use nuclear weapons against non-nuclear-weapon states or nuclear-weapon-free zones."[8] China has frequently called on the other nuclear powers to adopt an NFU policy. In the words of China's disarmament ambassador: "In the post-cold war era of today, it is obviously anachronistic to con-tinue with the policy of nuclear deterrence based on the first-use of nuclear weapons and thus subjecting other countries to nuclear threat."[9] China officially supports a goal of total nuclear disarmament by all nations but has stated it would only join Strategic Arms Reduction Talks (START) negotiations when the US and Russian stock-piles were reduced below the levels established by START II.[10]

Notwithstanding its official pronouncements, the actual nuclear doctrine of Beijing has been shrouded in an ambi-guity that may be deliberate.[11] The Chinese nuclear pos-ture is believed to be based on a countervalue second-strike capability[12] but may have evolved from a doctrine of "minimum deterrence" to one that envisages a limited war-fighting capability. The current consensus is that China's nuclear doctrine is best characterized by the concept of "limited deterrence," which is based on "communicating China's ability to inflict costly damage on the adversary at every rung on the escalation ladder."[13] Limited deterrence

"requires sufficient counterforce and countervalue tactical, theater, and strategic nuclear forces to deter the escalation of conventional or nuclear war. If deterrence fails, this capability should be sufficient to control escalation and to compel the enemy to back down."[14] China does not currently have all the capabilities to implement this concept but may be using it as a "wish-list of capabilities"—within budgetary and arms control constraints—from which to choose.[15] Limited deterrence capabilities—such as the need to improve strike accuracy—are likely framing China's current nuclear modernization program.

Delivery Systems

China relies on a strategic triad of delivery systems—land-based ballistic missiles, submarine-launched ballistic missiles (SLBM), and bombers. The primary delivery means is the land-based missile, the most capable system being the liquid-fueled Dongfeng (DF)-5A, known in the West as the CSS-4.[16] The DF-5A carries a payload of 3,200 kilograms and has a range in excess of 13,000 kilometers, making it capable of striking targets in the United States.[17] John Caldwell and Alexander T. Lennon write that "four missiles, each with one 3–5 megaton warhead, are currently deployed in hardened underground silos."[18] China has also developed a mobile solid-fuel missile, the DF-21, assessed to be capable of delivering a 200–300 kiloton warhead a distance of 1,800 kilometers.[19] Also, in the inventory is the short-range DF-15, known by its export designator M-9, assessed to be a "nuclear-capable, tactical missile with a maximum range of 600 kilometers."[20]

In the SLBM category, China developed the Julang-1 (JL-1) single-warhead missile with a payload of 200–300 kilotons and a range of 1,700 kilometers.[21] China's only ballistic missile submarine, the Xia, can carry 12 JL-1 missiles.[22] In terms of aircraft delivery systems, China has more than 100 H-6 medium bombers, of which at least 40 are believed to be nuclear-capable.[23]

Figure 1 summarizes the current inventory of Chinese nuclear delivery systems.

SYSTEM	QUANTITY
DF-5 ICBM	7
DF-4 ICBM	10
DF-3 IRBM	38
DF-21 IRBM	8
CSS-N-3 SLBM	12
DF-15	4
DF-11	?
H-6 Bomber	120
H-5 Bomber	200
SSBN	1

Source: *Jane's Defence Weekly*, 10 February 1999, in Anthony H. Cordesman, "China and the Asian Military Balance" (China database) (Monterey, Calif.: Center for Strategic and International Studies, March 1999), 51; and on-line, Internet, 27 March 1999.

Figure 1. Chinese Nuclear Delivery Systems

Modernization

As a result of reductions in the United States and Russian nuclear arsenals—which under START II will draw down to thirty-five hundred and three thousand respectively by the year 2003[24]—the Chinese nuclear arsenal has improved quantitatively. It is also taking steps to improve its force qualitatively. Beijing concluded a series of nuclear tests just before signing the Comprehensive Test Ban Treaty (CTBT) in 1996. Chinese officials claimed the tests were conducted to improve the safety and reliability of its nuclear arsenal, but it appears the tests were also motivated by Beijing's desire to develop smaller and more powerful nuclear weapons.[25] Added one source, "Smaller warheads are crucial to the development of a MIRV (multiple independently targeted reentry vehicle) capability, as well as to the development of more mobile missiles."[26] Concurrently, advances in solid-fuel technology will reduce launch

preparation time and improve the responsiveness of China's nuclear arsenal.[27]

China is making efforts to improve all three pillars of its strategic triad. Two land-based missiles, the DF-31 and DF-41, are under development and will give the Chinese a solid-fueled, road-mobile capability.[28] According to the National Air Intelligence Center, the DF-31—slated to be deployed around the year 2000—"will narrow the gap between current Chinese, US, and Russian ballistic missile designs."[29] These new missiles will slash launch-preparation times to less than 15 minutes for the DF-31 and less than five minutes for the DF-41, and they will be MRV-(multiple reentry vehicle) or MIRV-capable.[30]

China is also developing a second-generation submarine-launched ballistic missile, the 8,000-kilometer-range JL-2, which may be deployed on a new class of nuclear submarine.[31] With respect to the air-breathing leg of the triad, China is developing the H-7 (B-7) bomber and may also decide to modify SU-27s purchased from Russia to make them nuclear-capable.[32]

The immediate goal of these programs is to improve the accuracy, range, guidance systems, and control of China's strategic forces.[33] The ultimate objective—whether to strengthen a power-projecting great power or to buttress a "fortress China"—is subject to considerable debate.

Proliferation Concerns and Commitments

China's record on nuclear nonproliferation has been far from stellar, but Beijing has certainly "come a long way" in the last three decades. As Secretary of State Madeleine K. Albright recently noted: "On proliferation, China has progressed from advocating the spread of nuclear weapons to signing the Nuclear Nonproliferation Treaty [and] the Comprehensive Test Ban Treaty."[34] In the 1970s the US-USSR Strategic Arms Limitations Talks were denounced by China as a cover for the arms race between the superpowers.[35] By the 1980s Beijing appeared to begin to appreciate the advantages of free riding on the various arms control agreements between Moscow and Washington, as subsequent

accords reduced the superpowers' strategic forces, elimi-
nated their intermediate-range missiles, and limited their
antiballistic missile systems.[36] In the 1990s Beijing has
come to recognize that it derives both political and security
benefits from participating in multilateral negotiations to
control nuclear weapons.[37] China's gradual and growing
acceptance of international nonproliferation norms has been
due in large part to "U.S. sanctions, laws, and policies, as
well as positive inducements."[38] These inducements in-
clude recognition of China's major-power status by the in-
ternational community and "access to international trade,
capital, and technology."[39]

Before acceding to the Nuclear Nonproliferation Treaty
(NPT) in 1992, China provided assistance to the Pakistani
nuclear weapons program, which it saw as a balance to the
conventional and nuclear strength of its rival India.[40] A
1997 US Arms Control and Disarmament Agency report
warned that "Questions remain about contacts between
Chinese entities and elements associated with Pakistan's
nuclear weapons program."[41] China also assisted the Ira-
nian nuclear program under International Atomic Energy
Agency (IAEA) safeguards but has since agreed not to pro-
vide further nuclear assistance to that nation.[42] China's
support to the "peaceful" nuclear programs of Pakistan,
Iran, and Algeria has raised concern about dual-use appli-
cations of materiel and technology.[43] A May 1996 Pentagon
report notes that China's undermining of nonproliferation
goals stems primarily from "the role of Chinese companies
in supplying a wide range of materials, equipment and
technologies that could contribute to NBC [nuclear, bio-
logical, and chemical] weapons and missile programs in
countries of proliferation concern."[44]

China has recently taken meaningful steps toward be-
coming a responsible partner in the international nonpro-
liferation regime. A member of IAEA since 1983, China
acceded to the NPT in 1992. It also honored its commit-
ment to support a comprehensive ban on nuclear tests
(after completing a series of tests in 1996), becoming one of
the first signers of the CTBT that same year.[45] More re-
cently, China became a member of the Zangger Committee
in October 1997, joining other NPT states in agreeing not

to export items from a safeguard trigger list to facilities not under IAEA safeguards.[46] Beijing is not yet a member of the Missile Technology Control Regime (MTCR) but has entered into a bilateral agreement with the United States to abide by MTCR guidelines.[47]

There have been setbacks in China's growing coopera-tion, however, as in the case of alleged 1994–95 deliveries of ring magnets—used in uranium enrichment—to Paki-stan.[48] The Chinese government denied awareness of the transfers, indicating the possibility of a "center-periphery problem" where Beijing may not have specifically approved the initiative of a Chinese enterprise to export the mate-rial.[49] In the wake of considerable controversy and high-level negotiations, the United States decided not to respond with sanctions against China based on the following three factors:

(1) the finding that senior-level Chinese officials were unaware of the ring magnet transfer;
(2) China's new public commitment not to "provide assistance to unsafeguarded nuclear facilities"; and
(3) China's pledge to engage in a dialogue with the Unite d States on improving export controls.[50]

Recently, China sharply criticized the May 1998 Paki-stani and Indian nuclear tests, saying they "have not only seriously impeded international non-proliferation efforts, but have produced a grave impact on regional and world peace and stability."[51] Beijing has good reason to fear a nuclear arms race on her southern border, especially in light of her long-standing rivalry with India.

Other recent positive developments in nuclear nonprolif-eration cooperation include the following:

• China and the United States have jointly stated their intention to pursue negotiation of a fissile material cut-off treaty (October 1994).[52]
• China joined the other original nuclear powers in pro-viding positive security assurances to nonnuclear weapon states which are signatories of the NPT (April1995).[53]
• China and the United States reached an accord to de-target strategic nuclear weapons that had been

aimed at the other and to establish a hotline between the two capitals (June 1998). [54]

Implications for the United States

Unarguably, based on recent developments in Chinese nuclear nonproliferation cooperation, the United States has much with which to be satisfied. As described above, in addition to China's more complete integration into the international nonproliferation regime, the number of bilat- eral United States–China agreements in this arena has been growing. Despite the progress, however, there remain a number of areas of friction and divergence between the United States and China.

More to Do in Nonproliferation

China is not a member of the Nuclear Suppliers Group and does not require full-scope safeguards in the destina- tion country as a precondition for Chinese nuclear ex- ports.[55] There is also apprehension about Chinese sales of nuclear-related or destabilizing conventional arms to coun- tries with proliferation concerns. These include exports of such missiles and missile technology as the reported transfers of Chinese M-11 missiles to Pakistan.[56] In Prolif- eration: Threat and Response the Office of the Secretary of Defense maintains that "in most cases, Beijing agrees pub- licly on the danger and inadvisability of NBC weapons and missile proliferation." On the other hand, China's continu- ing and long-standing economic and security relationships provide incentives for activities that are inconsistent with some nonproliferation norms.[57]

Chinese Opposition to TMD/NMD

China is very concerned about potential deployments by the United States of theater missile defense (TMD) systems in East Asia as well as developments in the national mis- sile defense arena. Both of these will have the effect of undermining the deterrent value of China's nuclear arse- nal. In 1995 a Chinese official publicly reiterated Beijing's

long-standing opposition to the deployment of an advanced ballistic missile defense system as a development that would "trigger an arms race in outer space" and "increase the danger of nuclear war."[58] Beijing has also warned that the deployment of a TMD system would be met with an expansion in Chinese offensive systems.[59]

Modernization of China's Nuclear Arsenal

As described earlier, China's efforts to expand and modernize its nuclear arsenal are well under way. It should be noted that China is not constrained in these efforts by any arms control agreement (SALT, START, etc.), such as those governing the United States and Russia.[60] In fact, "as the United States and Russia reduce the size of their arsenals as mandated by the START treaties, improvements to China's nuclear weapons will mean that asymmetries between China's nuclear forces and those of the major nuclear powers will narrow."[61]

Regional Security

Some analysts warn of the adverse impact China's nuclear modernization efforts may have on the region. Beijing's assessment of its nuclear force requirements may be driven by such factors as stability on the Korean peninsula, Chinese concerns vis-à-vis Japan, the Indian-Pakistani dispute, and Taiwanese stirrings for independence.[62] Additionally, China's modernization efforts might stimulate a "nuclear modernization race" among neighboring countries, including India and Russia.[63]

Taiwan

Taiwan is one issue over which the interests of the United States and China seem destined to collide. On the one hand, the United States has long been committed to the security of Taiwan and is opposed to a resolution of the matter by force. The Chinese government, on the other hand, recently reaffirmed that "the issue of Taiwan is entirely an internal affair of China. . . . The Chinese govern-

ment seeks to achieve the reunification of the country by peaceful means, but will not commit itself not to resort to force [emphasis added]."[64]

Chinese "saber rattling" near Taiwan in 1996 evoked a quick and powerful show of force by the United States. However, a future similar scenario may involve an entirely different calculus and drive completely distinct results. As one analyst recently emphasized, "China's possession of a credible nuclear arsenal may provide a deterrent against any state seeking to intervene in the Taiwan Strait. . . . [W]ould the United States risk a nuclear confrontation over Taiwan with a more assertive, more capable China?"[65] There is also the risk that China's nuclear modernization efforts might convince Taiwanese leaders they need a nuclear program of their own.[66]

The Chinese Space Program

> Evidence is growing that the Chinese are working toward the launch of a domestic, manned spacecraft around the turn of the millennium.
>
> —Phillip Clark, "Chinese Designs on the Race for Space"
> Jane's Intelligence Review 9, no. 4 (April 1997)

A nation's prowess in space confers both prestige and power, and China has garnered a good measure of both in almost three decades of space activity. China's space program takes on special significance for the United States at the dawn of the twenty-first century, both because of the strategic advantages it confers to Beijing in the military realm and because of China's decision to open its space launches to international customers.

Satellite Launchers

China has been a space-faring nation since 1970, when it launched its first Dong Fang Hong ("East is Red") satellite using a Chang Zheng (CZ/"Long March") launch vehicle.[67] A more advanced vehicle, the CZ-2C, was first launched in 1975 and has become China's most utilized launcher.[68] It is capable of lifting 2,000 kilograms to low Earth orbit (LEO) and has been used with a recoverable microgravity

platform to return 150-kilogram payloads to Earth.[69] In 20 years of service, 14 of these two-stage vehicles were launched, with a 100-percent success rate.[70] In the 1980s the CZ-3 and CZ-4 launch vehicles, building on the CZ-2 design, added geosynchronous Earth orbit (GEO) and sun-synchronous capabilities to the Chinese launch program.[71] The CZ-3 launcher includes a cryogenic (very cold liquefied gases) third stage; with the first launch of this vehicle in January 1984, China became the third user—joining the US and the European Space Agency—of cryogenic propul-sion.[72] The CZ-3 can place 1,400 kilograms into geosyn-chronous transfer orbit or 5,000 kilograms into LEO and has achieved a 73-percent success rate.[73] The CZ-4 simi-larly grew out of predecessor launch vehicle programs. CZ-4 lift capability is advertised to be 2,500 kilograms to sun-synchronous orbit and 4,000 kilograms to LEO.[74] Two launches have been conducted since 1988, with 100 percent success.[75] The comparative dimensions of the CZ family of launch vehicles are shown in figure 2.

Chinese Satellites

Given China's information-restricted society, it is not surprising that open sources vary in precision about such details regarding the total number of satellite launches
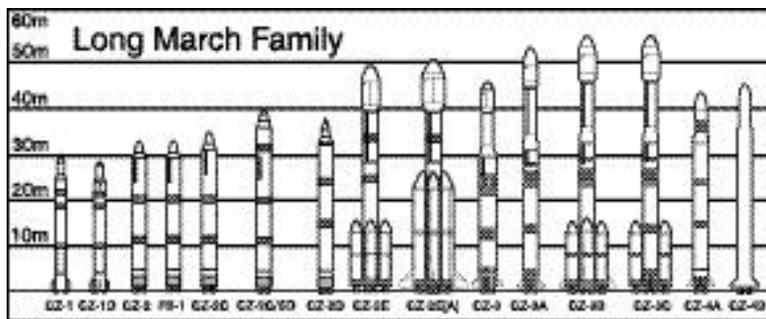
CHEN LAN

Source: Sketch downloaded from *Dragon in Space* Internet site, 15 December 1998.

Figure 2. Long March Launch Vehicles

conducted by China to date. The Air Force Association's Space Almanac sets the figure as "at least 50,"[76] while the Federation of American Scientists reports a total of 60 satellite launches by the Chinese, "of which 49 were completely successful, with another 7 failing to reach orbit and 4 suffering post-launch failures."[77] Jane's Space Directory itemizes 56 launches of 58 satellites between 1970 and 1996.[78]

Chinese satellites can be divided into three broad categories. The most numerous are the recoverable *Fanhui Shi Weixing* satellites, originally designed for photoreconnaissance but later modified to add a remote-sensing capability.[79] A second category of satellites includes those designed for communications, which China began launching in 1984.[80] The latest version—the *Dong Fang Hong 3*—was launched into geosynchronous orbit in May 1997 to provide voice and video communications.[81] Satellites designed for remote sensing and meteorology comprise the third category of Chinese satellites. Two *Feng Yun*-1 satellites launched into sun-synchronous orbit in 1988 and 1990 subsequently suffered problems in orbit, but the June 1997 launch of a *Feng Yun*-2 meteorological satellite into geosynchronous orbit was successful.[82] Additional test and scientific satellites have been launched throughout the length of the Chinese space program.

Chinese Launch Infrastructure

The Chinese space industry has three major launch complexes. The nation's first launch center was built at Jiuquan (40.6N/99.9E) in northern China. To avoid vehicle overflight of Russia and Mongolia, launches from that site are limited to a southeasterly direction into orbits between 57 and 70 degrees.[83] The Chinese have launched more than 25 satellites into low Earth orbit from Jiuquan since 1970.[84] Additionally, a new launch pad is being constructed at this site, reportedly to support a manned space flight program.[85] The Xichang launch center in south China (28N/102E) became operational in 1984 and is the nation's primary site for launches into geostationary orbit.[86] Xichang was also the site for China's first foreign

commercial launch (AsiaSat 1) in April 1990. [87] The nation's newest launch facility, Taiyuan, is located in northeastern China (38N/112E). Active since 1988, the site is used to launch satellites into polar orbit for remote-sensing, weather, and reconnaissance missions. [88]

Operations at these sites as well as telemetry, tracking, and commanding (TT&C) functions are performed by the China Satellite Launch and TT&C general organization, while the China Academy of Launch Vehicle Technology provides on-site launch supervision. [89] According to the Dragon in Space Internet site, the control and tracking network for China is comprised of the Beijing Aerospace Command and Control Center, Xian Satellite Control Center, numerous domestic tracking stations throughout China, an overseas tracking station located in the south Pacific on Kiribati, and three tracking ships. [90] The Federation of American Scientists identifies domestic tracking sites at the following locations: Changchun, Guiyang, Khashi, Minxi, Nanning, Weinan, Xiamen, and Yilan. [91]

Commercial Launch Services

After its first successful GEO launch in 1984, China began offering launch services to international customers. [92] The first foreign commercial launch took place in 1990. Among the companies that signed up for Chinese services are Intelsat, Globalstar, APStar, and EchoStar; [93] great international interest notwithstanding, the program has been plagued by several mission failures, including the 1996 loss of a US satellite. There have also been allegations of unfair pricing, leading to a 1988 agreement that limited Chinese launches to nine foreign satellites by the end of 1994. [94] The agreement was revised in 1995 to permit an additional 11 satellites to be put into GEO by the year 2001. [95] Provisions in the accord allow this figure to increase "if the annual global requirement is at least 20 satellites or if western [sic] vehicles cannot accommodate the market." [96]

With the expansion of space technology and the corresponding increase in the number of space-faring nations, competition for scarce launch capabilities is intense.

Worldwide, some seventeen hundred commercial satellite launches are projected to take place over the next 10 years, exacerbating the approximate three-year global backlog for launcher space.[97] With only three other competitors—the United States, Russia, and the European Union—on the supply side of space launches, the significance of China's commercial launch capability is evident.

Technology Transfer Issues

Then come US concerns about technology transfer to China, a potential future adversary, and known proliferator of advanced technologies to such "rogue states" as Iran and North Korea. The current controversy regarding US use of Chinese launchers stems from the February 1996 accident involving a US Loral/Intelsat satellite aboard a Long March (CZ) 3B launcher. Accident investigation documents given to the Chinese by the Loral Corporation may have contained sensitive guidance technology.[98] Consequently, the House of Representatives voted in May 1998 to ban exports of all US satellites to China because China could use the technology to upgrade its intercontinental ballistic missiles (ICBM).[99] Additionally, in the wake of the May 1998 nuclear tests in South Asia, Congress allocated $2.5 million to investigate technology transfers to China.[100]

Some of the furor surrounding this issue is likely related to antagonism over China's pricing of its Long March launches—reportedly some 30 percent cheaper than its US competitor.[101] However, given this country's limited space launch infrastructure and its focus on promoting national competitiveness and economic growth, the United States may have no realistic alternative but to allow its companies to take advantage of China's excess launch capacity.

Trends in the Chinese Space Program and Their Implications for the United States

Just as the doctrine and disposition governing China's nuclear program are shrouded in ambiguity, so too are the capabilities and military implications of China's space pro-

gram. Almost 20 years ago, a spokesperson for a US dele-
gation which had toured the Chinese space industry noted
the difference between that nation's actual and stated ca-
pabilities: "Their [China's] own frequently cited description
of their [space] technology as primitive is excessively mod-
est. Advanced but simple is more apt." [102]

While it is not unusual for civilian space programs to
have military applications, the program of China has been
described as "distinct in the degree of its military involve-
ment, the extent of its military functions, and the scale of
its military significance." [103] In fact, China's progress in its
space program has been linked closely to progress in its
ballistic missile program, with activities and tests in the former
used to advance objectives in the latter. [104]

At least five strategic objectives of the Chinese space
program can be identified:

(1) improve the accuracy of ICBM guidance systems;
(2) enhance the command, control, and communica-
    tions (C^3) of Chinese strategic forces;
(3) improve intelligence-gathering capabilities;
(4) provide early warning for Chinese civil and air de-
    fense; and
(5) lay the foundation for possible future capabilities in
    strategic defense. [105]

The Chinese appear to have been working towards ac-
quiring a manned space capability since the 1970s. [106] By
the late 1980s China had officially disclosed its intention
to launch a space shuttle by the year 2000 [107] and was
beginning to discuss a program for a limited space station. [108]

In 1990, after the first flight of its CZ-2E launcher,
China reportedly began to study a spacecraft that could be
launched onto that vehicle with four astronauts aboard. [109]
A 1995 ITAR-TASS news report stated China was seeking
to buy Russian equipment for use in a manned space pro-
gram—to be launched around the 2000–2002 time
frame—and that it also intended to build an orbital space
station around the year 2015. [110] One year later, the same
news agency reported two "Chinese cosmonauts" were un-
dergoing training in Russia for a mission on a Chinese
spacecraft, planned for 1999 to coincide with the 50th an-

niversary of the founding of the People's Republic of China.[111] A Russian defense analyst recently stated that the Chinese space shuttle program has been officially un-der way since 1992 and that the first launch is due in 2005 from a site on Hainan Island.[112] While the specifics remain unclear, the evidence points to a Chinese attempt to achieve a recurring manned presence in space within the decade.

As China's capabilities in the space industry have ad-vanced, so apparently has its determination to begin to "level the playing field" in this arena. Although Beijing re-cently officially reaffirmed its opposition to the develop-ment of antisatellite weapons,[113] a November 1998 Penta-gon report indicates the Chinese may be involved in exactly such an endeavor. The report warns that the Chinese may be building an antisatellite laser, possibly with assistance from scientists from the former Soviet Union.[114] Such ef-forts could lead to a weapon that could cripple orbiting US satellites.

Many analysts have emphasized the importance of the 1991 Gulf War in convincing China of its need for defense modernization. Lessons learned from that conflict appar-ently inspired the Chinese to abandon the 1980s-era strat-egy of fighting "a people's war under modern conditions" to one focused on fighting "modern warfare under high-tech conditions."[115] The need to upgrade China's command, control, communications, and intelligence (C^3I) system is now a top priority, and space-based assets are considered vital to that effort.[116] One example is a proposal to create a dedicated network for defense satellite communications, since the People's Liberation Army (PLA) currently has only limited access to China's six communications satellites.[117] Other Chinese efforts to prepare for high-tech wars of the future will be explored later.

It should be noted that China does not need to close the technological gap with the United States in a sequential manner. China has repeatedly demonstrated the ability to leapfrog over developmental stages in a number of select defense programs, a talent especially well suited for the current information age with its wealth of available tech-nology and data. Also international commercial services can help fill the gaps between current and desired capabili-

ties. For example, the Global Positioning System provides positioning and timing data to users around the globe— information with both navigational and targeting applications. Commercially available satellite imagery is also widely available from such systems as SPOT (satellite pour l'observation de la terre) and LANDSAT (land satellite). These two systems—with resolutions of 10 to 30 meters—clearly demonstrated their military utility during the Gulf War.[118]

Information Warfare, Chinese Style

A 1-ounce integrated-circuit chip in a computer will perhaps be much more useful than a ton of uranium.

—Wang Xusheng, Su Jinhai, and Zhang Hong
 "China: Information Revolution, Defense Security"
 Beijing Jisuanji Shijie [China Computerworld], 11 August
 1997, 12 January 1999

In the networked world of the future, every chip is a potential threat and every computer a potential weapon.

—US Embassy Beijing Report
 "PRC Computer Security Concerns Grow"

China's booming economy has allowed it to pursue selective modernization of its military capabilities, including certain conventional weapon systems and, as discussed already, its nuclear arsenal and space assets. In addition, Chinese strategists are studying a newly emphasized form of warfare that focuses on gaining and exploiting information, attacking the information available to an adversary, and defending against attacks on one's own information and information systems.

Chinese Views on Information Warfare

Operation Desert Storm has been described as the first "information war,"[119] and China is carefully studying the lessons learned from that conflict. While the Gulf War did not initiate Chinese thinking about future warfare, the conflict apparently stimulated the 1992 decision by PLA leaders to focus on preparing China's armed forces to wage high-tech warfare.[120] China not only gained an appreciation for high-tech weaponry, it also saw the need to mod-

ernize the PLA's C³I network and to expand the nation's space-based communication and navigational systems.[121] Chinese military analysts understand that information-age technologies have changed how wars are fought.

Shen Weiguang, a Chinese IW expert, notes that concerns about Chinese vulnerability to IW have grown in the past decade.[122] China's response has been vigorous and broadly focused. According to a recent China Defense News article, war games are used to train China's IW experts, Chinese military schools offer such courses as "IW Command and Control" and "IW Technology," and the ministry of education now offers a specialization in information warfare.[123] Further indicators are the appearance of specialized publications dedicated to the study of IW. In addition, the Chinese Academy of Sciences has established an "Information Security Engineering Center."[124]

A survey of Chinese military literature reveals the scope and depth of Chinese interest in information warfare. Maj Gen Wang Pufeng, former director of the strategy department of China's Academy of Military Science, describes the role of information warfare for the PLA: "In the near future, information warfare will control the form and future of war. We recognize this developmental trend. . . and see it has a driving force in the modernization of China's military and combat readiness. This trend will be highly critical to achieving victory in future wars."[125]

Shen Weiguang has also analyzed how IW affects military doctrine. The following examination of his main points indicates that Chinese military thinkers both grasp the tenets of IW and appreciate its inherent power: "Information power" gives a military unit its freedom of movement.

- IW targets focus on disrupting the enemy's decision-making process.
- IW makes surgical strikes possible.
- IW is a "high tech people's war"—to be waged from the home or office.
- In IW "front and rear are reversed"; civilian technicians may be the best soldiers.
- "Compared with nuclear weapons, information weapons are easier for small, weaker countries to obtain."

- "In the networked world of the future, every chip is a potential threat and every computer a potential weapon."[126]

Analysts from the PLA Academy of Electronic Technology summarized Chinese thinking in the field of information warfare in six concepts:

- The primary goal of IW is to attack the enemy's command and control systems.
- Information should be used to harass and confuse the enemy.
- IW tactics are to attack enemy commanders and headquarters at every level.
- The enemy's "eyes and ears" should be destroyed, while protecting one's own ability to see and hear.
- Information deception and concealment procedures, such as multi-node, multi-path, and multi-frequency network systems, should be used to ensure survivability.
- Weapons with imbedded information technology (IT) will become the "dominant factors on the battlefield. . . . IT will be used to carry out electronic warfare, command and control warfare, and warfare characterized by attacks with computer viruses."[127]

Chinese thinkers have highlighted the critical role of information in high-tech warfare and even assigned it the preeminent role in war. In Information Warfare and Training of Skilled Commanders, Lei Zhoumin describes information as a force multiplier and "a strategic resource more important than men, materials, and finances."[128] Chang Mengxiong, senior analyst in the Committee of Science, Technology, and Industry (COSTIND) Institute of Systems Engineering, predicts that in future high-tech wars, air and sea superiority will still be required, but information superiority will have to be won first.[129] He asserts that in twenty-first-century warfare, information warfare "will decide who will win and who will lose the war."[130] Other analysts concur that "the struggle to wrest information dominance will permeate everything and will be exceptionally fierce and intense."[131]

IW is understood to have both offensive and defensive applications. One military strategist maintains that a situation of "information offensive" would exist only for the side with superior technology.[132] For the side on the information defensive, tactics available would include counter-reconnaissance (either passive—e.g., deception and concealment, or active—such as blinding or destroying the adversary's reconnaissance systems), antijamming measures, virus protection, and information counterattack.[133]

Chinese military literature reflects concern about defensive counters to virus attacks. In an essay entitled "Exploration and Analysis of Military Computer Security and Virus Protection," Chou Hsi alleges the United States is developing a "computer virus weapons plan" that would plant viruses in computers and electrical equipment exported abroad—the virus would presumably be activated during a conflict to cause the equipment to malfunction.[134] His essay calls for China to take preventive measures against future IW attacks, including raising computer security awareness in the armed forces, creating security filters for imported electronic equipment, and conducting research on computer viruses.[135]

Chinese military thinkers are also addressing the offensive use of computer viruses to destroy or degrade adversary capabilities. In Information Warfare Poses Problems, Zhou Li and Bai Lihong assert: "Computer viruses can be used to track down the enemy's target system and the enemy's guided missiles may end up attacking the side which has launched them."[136] On this same issue, another analyst highlights the superiority of IW over traditional weapons of war: "Once a computer system is damaged so that it cannot operate normally, cruise missiles and other precision-guided weapons become arrows without targets; and high-performance aircraft, tanks, warships, radar, and activated command systems will be totally in the dark about what to do."[137]

In short, information warfare is seen as a phenomenon that is changing the nature of war from one focused on seizing territory or destroying forces, to one seeking to paralyze the adversary's information systems and to destroy his will to resist.[138]

Information Warfare with
Chinese Characteristics

Many of the principles of asymmetric warfare, including the foundation for information warfare, have been a part of Chinese thinking for over two millennia. Chinese strategists draw parallels between ancient wisdom and future warfare, relying on timeless prescriptions from such sources as Sun Zi's (Sun Tzu) The Art of War:

- Know your enemy and know yourself, and in a hundred battles you will not be in peril. [139]
- The supreme skill in war is to defeat the enemy without fighting. [140]
- Attack the enemy's strategy, then his alliances. [141]

Cultural Foundations

Chinese military planners are well aware of the wide gap that exists between the current state of their military technology and that of potential competitors such as the United States. Even while their nation takes steps to improve its relative position, Chinese strategists see in Sun Zi a prescription for the defeat of the strong by the weak. As the former director of the Strategy Department of China's Academy of Military Science recently noted: "In light of the fact that the military lags behind its strong enemies in information technology and information weapons, the military must emphasize the study of ways to use inferior equipment to achieve victory over enemies with superior equipment. 'Using the inferior to overcome the superior' is a tradition of China's military." [142]

These words capture the essence of the Chinese approach to asymmetric warfare. Sun Zi's exhortations to "stay clear of the enemy's main force and strike at its weak points," [143] and "the weak and the strong can shift their position" [144] are applicable to the Chinese military situation today. While in a position of relative military inferiority, Beijing may also draw on ancient Chinese wisdom to "hide one's capacities and bide one's time" to strengthen its power. [145]

The wisdom of Sun Zi also underpins China's classic deterrence strategy: "The national security deterrence per-

ception of 'overawing the enemy' is the important means to achieve the aim of 'subduing the enemy without fighting.'"[146] This concept is easily extended to the information realm; in fact, information deterrence may be the strongest suit in the Chinese inventory against an information-dependent adversary like the United States. COSTIND's Mengxiong maintains that, given two unequal opponents, "if one side can effectively weaken the information capability of the other side, even if its capability in other ways is less, the other side will dare not take any ill-considered action."[147]

Chinese military strategists continue to study the transformation of the US military in the wake of the Gulf War. Since the United States is seen to be at the pinnacle of advances in high-tech warfare, the Chinese are analyzing the thinking of US futurists, revisions in US military doctrine, C^{3}I, and organizational restructuring, etc.[148] The Chinese have a long tradition of adapting outside thinking to fit their needs. Martin C. Libicki, a US information warfare expert, notes that militaries prosper by adapting ideas to their specific circumstances and strategies, saying,[149] "We know the Chinese can copy our thoughts, but whether they can innovate in pursuit of their own objectives is not yet obvious."[150] Indian analyst M. Ehsan Ahrari responds with this warning: "The Chinese have proven themselves remarkable in indigenizing Marxism to suit their cultural requirements and they are likely to develop information-based warfare techniques to suit their special needs before too long. The USA must remain especially sensitive to this profound historical reality about the PRC."[151]

In a work entitled America, Russia and the Revolution in Military Affairs, two young Chinese officers at the Academy of Military Science have issued their own warning: "Those who believe that the current revolution in military affairs will be under the control of the United States or can develop only according to the speed and directions set by the United States are extremely wrong and quite dangerous."[152] Chinese attempts to "set the speed and directions" for the development of a unique information warfare capability may be well under way. For example, some PRC strategists have attempted to wed the traditional Maoist idea of a "people's war" with the special nature of informa-

tion warfare, creating the specter of "information warfare with Chinese characteristics."

People's Information War and the Internet—Is There a Connection?

While evolving from a strategy of "fighting a people's war under modern conditions" to one of "fighting modern warfare under high-tech conditions,"[153] the PLA has not lost its appreciation for the force to be generated by mobilizing China's vast human resources, saying that "In the people's war, no great significance is attributed to the differentiation between military and civilian realms, between military personnel and civilians."[154] This approach is boosted by access to information technology: "Thanks to the widespread availability of computers, there are increasing opportunities for individuals as well to actively take part in an information war. . . . We can drop into a café where a computer provides us with a wide variety of news and messages; in precisely the same way, thanks to special software and hardware, we are capable of destroying an enemy's data banks and information networks."[155] Other statements by Chinese military thinkers echo this view:

- "[A]nybody who understands computers may become a 'fighter' on the network."[156]
- "The development of the Internet opens up new opportunities for the individual to participate directly in an information war."[157]
- "[A]ll preconditions are in place for information warfare to be not simply a matter left up to armed forces, but rather one in which the general public can take part."[158]

In Exploring Ways to Defeat the Enemy Through Information, Cai Renzhao calls for the military and civilians to cooperate in "tapping the military potential of the 'information superhighway.'"[159] His strategy is echoed by the previously cited analysts of the PLA Academy of Electronic Technology: "Computer networks form the foundation for IW. IW is warfare waged by all the people under high-tech conditions. It is waged not only with military forces, but also with the aid of networks throughout society as a whole."[160]

Recognizing the multiplier effect of information technol-
ogy on both the national economy and the national de-
fense, several analysts have called for the nation to "build
an information superhighway network with distinctively
Chinese characteristics."[161] These "high-speed, high-capacity,
broadband information" networks would serve both the "mar-
ket" and the "battlefield."[162]

China's telecommunications infrastructure, currently sec-
ond in size only to that of the United States,[163] has under-
gone significant expansion and modernization in recent
years. A small but growing portion of the Internet, China
has four major state-approved networks connected directly
to the net. The status of the networks as of December 1996
is depicted in figure 3. With the Internet now "linking 1.2
million of the 20 million computers in China,"[164] Beijing
appears to have made a conscious decision to loosen re-
strictions on access to global information. Since economic
modernization is China's top priority, Beijing may be will-
ing to gamble with the political risks of broad Internet
access to reap the benefits of increased exposure to West-
ern information, especially in the scientific and technologi-
cal realms.

Loosening restraints on access to the Internet is also a
means to increase the technological sophistication of both
workers and soldiers. A growing population of skilled com-
puter users—with access to an unprecedented quality and
quantity of information on potential adversaries (across the
spectrum of economic, diplomatic, and military confronta-
tion)—is the pool of China's future military leaders and
information warriors.

Implications for the United States

The United States is the most advanced nation in the
world in cyberspace, but the dilemma for the Pentagon is
that it may also be the nation most vulnerable to attacks in
that arena.[165]

The autumn 1996 edition of Parameters outlines the ba-
sic features of strategic information warfare. These include
low cost for the aggressor, difficult warning and attack
assessment problems, complications in building and sus-

taining coalitions in an IW environment, and the vulner-
ability of the US homeland. [166] All four of these elements
appear to be favorable for Chinese use of IW.

First, an extraordinarily low investment can result in
tremendous capability. As the director of the National Se-
curity Agency (DIRNSA) recently stated in congressional
testimony, "Anyone with a computer, modem, and tele-
phone line can make use of a burgeoning array of network
sniffers, malicious software, and sophisticated information
attack tools to disrupt network operations." [167] He also
maintained that "a moderately sophisticated adversary can
cause considerable damage with fewer than thirty people
and a nominal amount of money if the systems they are
attacking are not adequately protected and defended." [168]
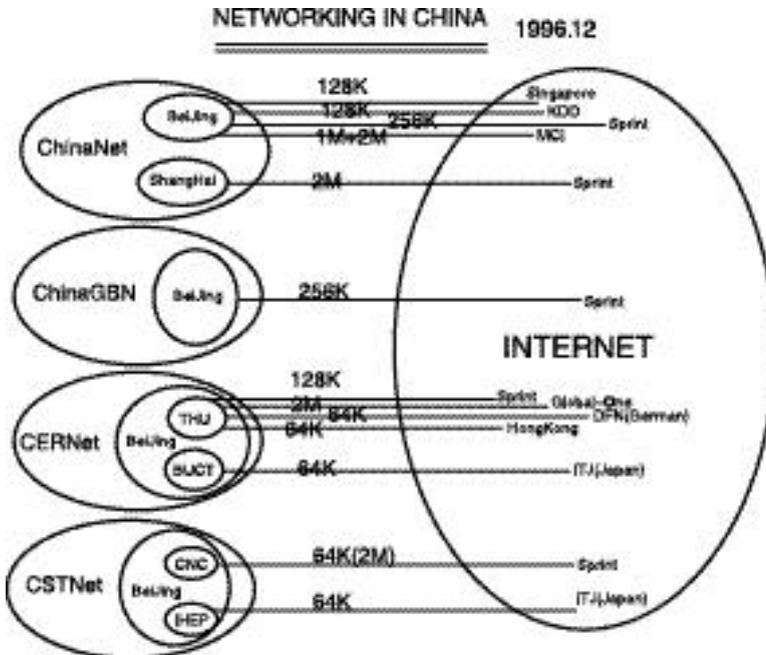
Source: Xu Rongsheng, "Internet Development in China" (in Chinese), February 1998.

Figure 3. Chinese Network Connectivity with the Internet (December 1996)

Furthermore, new hacker tools are constantly under development, widely disseminated, and available in open forum.[169] In the words of Chinese IW expert Shen Weiguang, "the information to attack the net is available on the net."[170]

Second, attacks against US systems are widespread and difficult to trace. A 1996 Department of Defense report estimated that a quarter of a million network attacks against US defense systems occurred during the previous year.[171] Even more disturbing is the fact that, according to DIRNSA, "even when attacks are detected and reported, we rarely know who the attacker was."[172] In the words of a Chinese author, "an information war is inexpensive, as the enemy country can receive a paralyzing blow through the Internet, and the party on the receiving end will not be able to tell whether it is a child's prank or an attack from its enemy."[173] Such a situation would work to China's advantage, should it choose to strike at US vulnerabilities while taking advantage of ambiguity to avoid retaliation.

Third, IW is an ideal weapon to dissuade an adversary's ally from joining a hostile coalition. In a hypothetical scenario, if China were to use a limited information attack to demonstrate its capability to take down the Japanese financial system, Tokyo might well think twice about supporting US operations in a regional confrontation. Recall Sun Zi's emphasis on the importance of disrupting alliances.

Fourth, the US homeland itself is vulnerable to an IW attack. The director of the Central Intelligence Agency (CIA), George Tenet, recently predicted the Information Age battlespace will include the US domestic infrastructure, with electric power grids and telecommunications networks "targets of the first order."[174] To illustrate his point, Director Tenet quoted an article in the China's People Liberation Daily that stated that "an adversary wishing to destroy the United States only has to mess up the computer systems of its banks by high-tech means. This would disrupt and destroy the US economy."[175] Tenet further noted the following:

> As I recently testified before the Senate Intelligence Committee in January [1998], we have identified several countries that have government-sponsored information warfare programs. Foreign nations have begun to include information warfare in their military doctrine, as well as their war college curricula, with respect to both defensive and

offensive applications. It is clear that nations developing these programs recognize the value of attacking a country's computer systems, both on the battlefield and in the civilian arena. The magnitude of the threat from various forms of intrusion, tampering, and delivery of malicious code, is extraordinary [emphasis in original].[176]

The DIRNSA differentiated between two types of IW threats: unstructured threats (random and limited) and structured threats (methodical, well supported, extensively funded, with long-term goals).[177] Lt Gen Kenneth Minihan believes that "the Chinese present a good example of the structured threat. In 1995 the Chinese military openly ac-knowledged that attacks against financial systems could be a useful asymmetrical weapon. By 1997 the Chinese military had incorporated computer warfare into an exer-cise scenario."[178]

The directors of both the CIA and NSA further concurred in outlining the risk that an adversary would turn to IW as a means of asymmetric warfare to level the playing field in a military confrontation with the United States.[179] If China chose to employ information attacks against US systems, it could achieve success both by concealing the identity of the attacker and by striking a blow against a US vulner-ability.

Of course, the preferred Chinese strategy would be to defeat the enemy without fighting. In this regard, it would seem the Chinese would have their choice of stratagems to employ: "hide one's capabilities" or "overawe the enemy." Either lever of "information deterrence" could serve to deter a potential adversary such as the United States from engaging it in war and may serve China well in the coming decades.

Conclusion

Hide one's capacities and bide one's time to strengthen one's power.

—Quoted in Yu Rubo and Qui Jianmin, "Philosophical Reflection on the Strategic Guideline of 'The Weak Can Defeat the Strong' in Ancient China," in The 4th International Symposium on Sun Tzu's Art of War, paper abstract (Beijing, 1988)

A collision of interests between the United States and China is inevitable. The question is not whether the two nations will collide but when and how. Already, bilateral relations have been strained and tested over such issues as human rights, intellectual property, and weapons proliferation. Will a more confident and militarily capable China be more willing to take on the United States over what it perceives as threats to its vital interests, such as the status of Taiwan and PRC claims in the South China Sea? A fundamental goal of the United States currently is to prevent the rise of a single dominant power in northeast Asia. It is not inevitable that the United States—in 15 years and beyond—will be in the position to maintain this goal and back it up with the credible threat of force in the region.

China has the potential to become a peer competitor of the United States. China's emergence as a great power seems almost inevitable when one considers its diplomatic strength, economic growth, natural resources—including its immense population—and its military potential, including the nuclear "card." To this, one must add China's advances in its nuclear and space capabilities. The eventuality and timing of such a scenario cannot be predicted with certainty. Factors that would tend to favor China's rise include sustainment of its economic growth, internal political stability, ability to address the domestic needs of a developing country, regional stability, and avoidance of military conflict in the near term with the United States.

US military advantages over China are narrowing in such critical areas as nuclear weapons, space technology, and information warfare. With its ongoing modernization program, China is developing nuclear weapons with increased accuracy, mobility, and range. In addition to these qualitative improvements, the Chinese arsenal will be in a better relative position quantitatively due to ongoing US and Russian strategic arms reductions. Beijing's growing prowess in space—including a possible manned presence in space within the decade—will also provide tremendous benefits in the military realm. In these areas and in information technology as a whole, China has been a beneficiary of the so-called technology paradox: the further technology advances, the easier it is to catch up. [180] Through concerted

effort and investment, China has demonstrated its ability in several areas to leapfrog over some of the evolutionary stages followed by advanced nations in developing its strategic capabilities. Beijing continues to leverage global advances in technology and communications to improve its own systems and/or upgrade its inventories at a fraction of the development costs incurred by other nations.

China's rapid economic growth supports technological modernization, and both go hand-in-hand with an improved defense posture. This is the case both because an expanding economy creates more money for direct investment in the military (if the political leaders so choose) and because of the opportunities to leverage dual-use (civilian and military) technology and infrastructure, such as electronics and space technology. An excellent example is Beijing's investment in the nation's telecommunications infrastructure—the expanding and modernizing network advances both commercial and military aims.

China does not (philosophically or militarily) have to approach US levels of capability or proficiency to pose a threat to the United States. There is strong evidence the Chinese are vigorously analyzing, pursuing, and acquiring the means to wage asymmetric warfare against a more powerful adversary. Even in the near term, reliance on asymmetric warfare could help Beijing level the playing field with the United States. It would be dangerous to draw parallels to "prove" Chinese military inadequacy far into the future. "Warfighting with Chinese characteristics" could be unrecognizable to a Western foe expecting an alter ego adversary. Asymmetric warfare can be cheap, low tech, readily available, and devastatingly effective. US advantages in military capabilities based on space and information systems have increased US reliance on these assets and correspondingly increased its vulnerabilities to their degradation or destruction. Reported Chinese research in antisatellite systems and China's progress in information warfare capabilities may allow it to stand up successfully to a technologically advanced adversary.

Information warfare may be the weapon of choice for China to use against a capable military adversary. There would be little reason for a hostile China to confine IW

attacks to military targets. In fact, the US civilian infrastructure—the power grid, telecommunications infrastructure, financial systems, emergency systems, etc.—is vulnerable. So are the infrastructures of US allies in the region. The shared knowledge of this fact may permit China to employ a strategy of information deterrence in a situation of confrontation with the United States. This is in keeping with two-millennia-old Chinese stratagems that advocate defeating the enemy without fighting. Alternatively, it could choose to wage IW, employing its traditional strategy of using the inferior to overcome the superior. Consistent with the principles of Sun Zi, an IW attack could be carried out with complete surprise and with sufficient deception to potentially avert a devastating counterattack.

It is not inevitable that China will become an adversary of the United States; however, such a possibility could become a self-fulfilling prophecy if the United States "mishandles" its relationship with China. A US policy of constructive engagement appears to offer more prospects for peaceful coexistence than attempts to contain China, which seem destined to fail. Beijing has repeatedly demonstrated its ability to develop or acquire the technology it needs to progress technologically. Attempts to isolate or contain China are likely to backfire, since the United States would lose both influence and leverage, and the action would simply invite responses ranging from indigenous solutions to reliance on non-US suppliers for critical technology and components. Although concerted efforts of a powerful country like the United States could slow Chinese progress in "sensitive" areas, the globalization of technology and profit motivations of other players effectively conspire to remove the technology "veto" from any one actor's hands. The United States holds some of the cards with which to positively shape the future of Sino-US relations—the specter of a militarily capable and potentially hostile China makes a compelling case for doing so.

<div align="center">Notes</div>

1. "China's Nuclear Testing" (China database) (Monterey, Calif.: Center for Nonproliferation Studies, November 1998), n.p.; and on-line,

Internet, 27 November 1998, available from http://cns.miis.edu/db/china/testpos.htm.

2. **Tracking Nuclear Proliferation, 1998: China (China database)** (Washington, D. C.: Carnegie Endowment for International Peace, 1998), 10; on-line, Internet, 11 November 1998, available from http://ceip.org/programs/npp/china/htm; "China's Nuclear Stockpile and Deployments" (China database) (Monterey, Calif.: Center for Nonproliferation Studies, November 1998), n.p.; and on-line, Internet, 27 November 1998, available from http://cns.miis.edu/db/china/ nforce.htm.

3. "China's Nuclear Stockpile and Deployments."

4. **Proliferation: Threat and Response** (Washington, D. C.: Government Printing Office, November 1997), 10.

5. Alastair Iain Johnston, "China's New 'Old Thinking': The Concept of Limited Deterrence," **International Security** 20, no. 3 (Winter 1995–96): 36.

6. John Caldwell and Alexander T. Lennon, "China's Nuclear Modernization Program," **Strategic Review** 28, no. 4 (Fall 1995): 28.

7. Information Office of the State Council of the People's Republic of China, "China's National Defense," **Beijing Review** 41, no. 32 (10–16 August 1998): 16.

8. Ibid., 30.

9. "China's Attitude Toward Nuclear Deterrence" (China database) (Monterey, Calif.: Center for Nonproliferation Studies, November 1998), n.p.; and on-line, Internet, 27 November 1998, available from http://cns.miis.edu/db/china/npolicy.htm.

10. M. Ehsan Ahrari, "Sino-Indian Nuclear Perspectives: So Close, Yet So Far Apart," **Jane's Intelligence Review** 10, no. 8 (August 1998): 31.

11. "China's Nuclear Doctrine" (China database) (Monterey, Calif.: Center for Nonproliferation Studies, November 1998), n.p.; and on-line, Internet, 27 November 1998, available from http://cns.miis.edu/db/china/npolicy.htm.

12. Ibid.

13. Johnston, 41.

14. Ibid., 5–6.

15. Ibid., 6, 38.

16. Caldwell and Lennon, 28.

17. Ibid.

18. Ibid.

19. Ibid.

20. Ibid., 29.

21. Ibid.

22. Ibid.

23. **Jane's Sentinel: China and Northeast Asia** (Coulsdon, Surrey, U.K.: Jane's Information Group Limited, 1998), 1.10.5.

24. Banning N. Garrett and Bonnie S. Glaser, "Chinese Perspectives on Nuclear Arms Control," **International Security** 20, no. 3 (Winter 1995/96): 72.

25. Ibid., 55.

26. "Nuclear Warhead Modernization" (China database) (Monterey, Calif.: Center for Nonproliferation Studies, November 1998), n.p.; on-line,

Internet, 27 November 1998, available from http://cns.miis.edu/db/china/wnwmdat.htm.

27. Caldwell and Lennon, 30.

28. Ibid.

29. Bill Gertz, "The Chinese Buildup Rolls On," Air Force Magazine 80, no. 9 (September 1997): 81.

30. "Nuclear Delivery System Modernization" (China database) (Monterey, Calif.: Center for Nonproliferation Studies, November 1998), n.p.; and on-line, Internet, 27 November 1998, available from http://cns.miis.edu/db/china/wnwmdat.htm.

31. Caldwell and Lennon, 30.

32. Ibid., 31.

33. Ibid., 30.

34. Madeleine K. Albright, "The Testing of American Foreign Policy," Foreign Affairs 77, no. 6 (November/December 1998): 57.

35. Garrett and Glaser, 47.

36. Ibid.

37. Ibid.

38. Tracking Nuclear Proliferation, 1998: China, 4.

39. Ibid., 5.

40. Proliferation: Threat and Response, 12.

41. Tracking Nuclear Proliferation, 1998: China, 3.

42. Proliferation: Threat and Response, 12.

43. Caldwell and Lennon, 34.

44. Tracking Nuclear Proliferation, 1998: China, 2.

45. "China's National Defense," 30.

46. Proliferation: Threat and Response, 11.

47. Ibid., 12.

48. Tracking Nuclear Proliferation, 1998: China, 7.

49. Mitchel B. Wallerstein, "China and Proliferation: A Path Not Taken?" Survival 38, no. 3 (Autumn 1996): 64.

50. Tracking Nuclear Proliferation, 1998: China, 7.

51. "China's National Defense," 29.

52. "US-China Convergence and Friction on Arms Control/Nonproliferation Issues" (China database) (Monterey, Calif.: Center for Nonproliferation Studies, November 1998), n.p.; and on-line, Internet, 27 November 1998, available from http://cns.miis.edu/db/china/index 1fr.htm; and "China's National Defense," 30.

53. Ibid.

54. "China's National Defense," 26.

55. "US-China Convergence and Friction on Arms Control/Nonproliferation Issues."

56. Ibid.

57. Proliferation: Threat and Response, 12.

58. Garrett and Glaser, 73.

59. Hans Binnendijk and Ronald N. Montaperto, eds., Strategic Trends in China (Washington, D. C.: National Defense University Press, 1998), 21.

60. Garrett and. Glaser, 43.

61. Caldwell and Lennon, 32.

62. Ibid., 33.

63. Ibid.

64. "China's National Defense," 15.

65. Caldwell and Lennon, 34.

66. Ibid.

67. "Overview of Chinese Satellite," Dragon in Space, August 1998, n.p.; and on-line, Internet, 10 September 1998, available from http://www.geocities.com/CapeCanaveral/Launchpad/1921/satellite.htm.

68. Phillip Clark, ed., Jane's Space Directory (Coulsdon, Surrey, U.K.: Jane's Information Group Limited, 1997), 210; and Space Warfare Center, Space Reference Guide (Falcon AFB, Colo.: 1998), 10–19.

69. Ibid.

70. Clark, 211.

71. Ibid., 208.

72. Space Reference Guide, 10–20.

73. Clark, 212.

74. Space Reference Guide, 10–21.

75. Clark, 213.

76. Tamar A. Mehuron, "Space Almanac," Air Force Magazine 81, no. 8 (August 1998): 39.

77. John Pike, "Chinese Space Launch Vehicles, World Space Guide, September 1998, n.p.; and on-line, Internet, 1 September 1998, available from http://www.fas.org/guide/china/launch.

78. Clark, 11.

79. Ibid.

80. Ibid.

81. "Launch History Search Results," Mission and Spacecraft Library, September 1998, n.p.; and on-line, Internet, 1 September 1998, available from http://www.leonardo.jpl.nasa.gov/cgi.bin.

82. Clark, 12.

83. Ibid., 459.

84. Ibid., 11.

85. "Launch and Research Facilities," Dragon in Space, July 1998, n.p.; and on-line, Internet, 10 September 1998, available from http://www.geocities.com/CapeCanaveral/Launchpad/1921/launch.htm.

86. Space Reference Guide, 10–18.

87. Clark, 12, 460.

88. Ibid.

89. Ibid., 454.

90. "Launch and Research Facilities."

91. John Pike, "Chinese Space Facilities," World Space Guide, September 1998, n.p.; and on-line, Internet, 1 September 1998, available from http://www.fas.org/guide/china/launch.

92. Clark, 10.

93. Ibid.

94. Ibid., 209.

95. Ibid.

96. Ibid.

97. Michael Hirsh, "The Great Technology Giveaway," Foreign Affairs 77, no. 5 (September/October 1998): 4.

98. Joseph Anselmo, "China Controversy Has Complex Roots," Aviation Week and Space Technology, 1 June 1998, 23.

99. Ibid., 24.

100. Hirsh, 2.

101. Anselmo, 24.

102. Chong-Pin Lin, China's Nuclear Weapons Strategy (Lexington, Mass.: Lexington Books, 1988), 55–56.

103. Ibid., 54.

104. Ibid.

105. Ibid., 55.

106. Phillip Clark, "Chinese Designs on the Race for Space," Jane's Intelligence Review 9, no. 4 (April 1997): 178–79.

107. Chong-Pin Lin, 54.

108. Clark, "Chinese Designs on the Race for Space," 179.

109. Ibid.

110. Ibid., 180.

111. Ibid.

112. Viacheslav A. Frolov, "China's Armed Forces Prepare for High-Tech Warfare," Defense and Foreign Affairs Strategic Policy 26, no. 1 (January 1998): 7.

113. "China's National Defense," 31.

114. "China May Seek Satellite Laser, Pentagon Warns," Los Angeles Times, 28 November 1998, in Air Force Space Command Legislative Up-date, 10 December 1998.

115. Frolov, 7.

116. Ibid.

117. Ibid.

118. Steve Berner, "Proliferation of Satellite Imaging Capabilities: Developments and Implications," in Fighting Proliferation: New Concerns for the Nineties, edited by Henry Sokolski (Maxwell AFB, Ala.: Air University Press, September 1996), 120.

119. M. Ehsan Ahrari, "Chinese Prove to Be Attentive Students of Information Warfare," Jane's Intelligence Review 9, no. 10 (October 1997): 469.

120. Frolov, 7.

121. Ibid., 7–8.

122. "PRC Computer Security Concerns Grow," 3.

123. Ibid.

124. Ibid.

125. Wang Pufeng, "The Challenge of Information Warfare," in Chinese Views of Future Warfare, ed. Michael Pillsbury (Washington, D. C.: National Defense University Press, March 1997), 318.

126. "PRC Computer Security Concerns Grow," 3.

127. Wang Xusheng, Su Jinhai, and Zhang Hong, "China: Information Revolution, Defense Security," Beijing Jisuaji Shijie (China Computer-world), (11 August 1997):1–2; and on-line, Internet, 12 January 1997, available from http://www.infowar.com/mil_c4I_121897a.html-ssi.

128. Ahrari, "Chinese Prove to Be Attentive Students of Information Warfare," 471.

129. Chang Mengxiong, "Weapons of the 21st Century," in Chinese Views of Future Warfare, 255.

130. Ibid.

131. Wang Baocun and Li Fei, "Information Warfare," in Chinese Views of Future Warfare, 337.

132. Wang, "The Challenge of Information Warfare," in Chinese Views of Future Warfare, 322.

133. Ibid., 322–23.

134. Ahrari, "Chinese Prove to Be Attentive Students of Information Warfare," 473.

135. Ibid.

136. Ibid.

137. Ch'en, "The Third Military Revolution," in Chinese Views of Future Warfare, 395.

138. Ibid., 393.

139. Sun Tzu, The Art of War, trans. Samuel B. Griffith (Oxford, U.K.: Oxford University Press, 1963), 84.

140. Ibid., 77.

141. Ibid., 78.

142. Wang, "The Challenge of Information Warfare," in Chinese Views of Future Warfare, 319.

143. Quoted in Jiang Lei, "Influence of Sun Zi's Concept of 'Attacking the Enemy's Strategy and Disrupting its Alliance' on the Current Non-Symmetric Strategy," in The 4th International Symposium on Sun Tzu's Art of War, paper abstract (Beijing: 1998), 94.

144. Quoted in Li Wenqing, "Carry Forward Sun Zi's Concepts and Seek Better Strategy to Subdue the Enemy in High-Tech Wars," in The 4th International Symposium on Sun Tzu's Art of War, 100.

145. Quoted in Yu Rubo and Qui Jianmin, "Philosophical Reflection on the Strategic Guideline of 'The Weak Can Defeat the Strong' in Ancient China," in The 4th International Symposium on Sun Tzu's Art of War, 101.

146. Yu Shifu, Han Xiaoling, and Zhang Qinbin, "On the Outlook of National Security Strategy in the Sun Zi and our National Security Strategy," in The 4th International Symposium on Sun Tzu's Art of War, 82.

147. Ibid.

148. Ahrari, "Chinese Prove to Be Attentive Students of Information Warfare," 471–72.

149. Ibid., 473.

150. Ibid.

151. Ibid.

152. Zhu Xiaoli and Zhao Xiaozhu, quoted in Chinese Views of Future Warfare, xxxiv.

153. Frolov, 7.

154. Wei Jincheng, "The People's Information War," in Infowar, eds. Gerfried Stocker and Christine Schopf (New York: Springer, 1998), 87.

155. Ibid., 90.

156. Wei Jincheng, "Information War: A New Form of People's War," in Chinese Views of Future Warfare, 409–10.

157. Wei Jincheng, "The People's Information War," 91.

158. Ibid., 92.

159. Ahrari, "Chinese Prove to Be Attentive Students of Information Warfare," 471.

160. Wang Xusheng, Su Jinhai, and Zhang Hong, "China: Information Revolution, Defense Security," 2.

161. Ibid., 5.

162. Ibid.

163. "PRC Internet: Cheaper, More Popular and More Chinese," US Embassy Beijing Report, October 1998, n.p.; on-line, Internet, 10 January 1999, available from http://www.usembassy-china.org.cn/english/sandt/Inetcawb.htm, 4.

164. Ibid.

165. "Information Warfare: A Two-Edged Sword," Rand Report, Fall 1995, n.p.; on-line, Internet, 12 January 1999, available from http://www.rand.org/publications/RRR/RRR.fall95.cyber/infor_war.html, 1.

166. Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson, "Strategic Information Warfare: A New Face of War," Parameters 26, no. 3 (Autumn 1996): 86.

167. Lt Gen Kenneth Minihan, quoted in US Congress, Senate Governmental Affairs Committee, "Vulnerabilities of the National Information Infrastructure" (24 June 1998). Text from Federal Information Systems Corporation Federal News Service, 24 June 1998, available from Congressional Universe, on-line, Congressional Information Service, 2.

168. Ibid., 3.

169. Ibid., 2.

170. "PRC Computer Security Concerns Grow," 4.

171. Sen. Fred Thompson (R-Tenn.), quoted from US Congress, Senate Governmental Affairs Committee, "Weak Computer Security in Government." Text from Federal Information Systems Corporation Federal News Service, 24 June 1998, available from Congressional Universe, on-line, Congressional Information Service, 2.

172. Minihan, 4.

173. Wei, "Information War: A New Form of People's War," in Chinese Views of Future Warfare, 411.

174. George Tenet, quoted in Senate Governmental Affairs Committee, "Weak Computer Security in Government," 24 June 1998. Text from Federal Information Systems Corporation Federal News Service, available from Congressional Universe, on-line, Congressional Information Service, 5.

175. Ibid.

176. Ibid., 4.

177. Minihan, 3.

178. Ibid.

179. Tenet, 5; and Minihan, 2.

180. Ahrari, "Chinese Prove to Be Attentive Students of Information Warfare," 471.

Glossary

C³I	Command, Control, Communications, and Intelligence
CALT	China Academy of Launch Vehicle Technology
CIA	Central Intelligence Agency
COSTIND	Committee of Science, Technology, and Industry
CTBT	Comprehensive Test Ban Treaty
CZ	Chang Zheng (Long March)
DF	Dongfeng
DIRNSA	Director, National Security Agency
GEO	Geosynchronous Earth Orbit
IAEA	International Atomic Energy Agency
ICBM	Intercontinental Ballistic Missile
IRBM	Intermediate Range Ballistic Missile
IT	Information Technology
IW	Information Warfare
JL	Julang
LANDSAT	Land Satellite
LEO	Low Earth Orbit
MIRV	Multiple Independently Targeted Reentry Vehicle
MRV	Multiple Reentry Vehicle
MTCR	Missile Technology Control Regime
NFU	No First Use
NMD	National Missile Defense
NPT	Nuclear Nonproliferation Treaty
NSA	Negative Security Assurance
NSG	Nuclear Suppliers Group
PLA	People's Liberation Army
PRC	People's Republic of China
SALT	Strategic Arms Limitation Talks
SLBM	Submarine Launched Ballistic Missile
SPOT	Satellite Pour l'Observation de la Terre
SSBN	Ballistic Missile Submarine
START	Strategic Arms Reduction Talks
TMD	Theater Missile Defense
TT&C	Telemetry, Tracking, and Commanding