MANEKSHAW PAPER No. 20, 2010

'Informationising' Warfare: China Unleashes the Cyber and Space Domain

Monika Chansoria

Centre for Land Warfare Studies
New Delhi

KNOWLEDGE WORLD
KW Publishers Pvt Ltd
New Delhi

Centre for Land Warfare Studies
RPSO Complex, Parade Road, Delhi Cantt, New Delhi 110010
Phone: +91.11.25691308 Fax: +91.11.25692347
email: landwarfare@gmail.com website: www.claws.in

The Centre for Land Warfare Studies (CLAWS), New Delhi, is an autonomous think tank dealing with national security and conceptual aspects of land warfare, including conventional and sub-conventional conflicts and terrorism. CLAWS conducts research that is futuristic in outlook and policy-oriented in approach.

ISBN 13: 978-93-80502-32-8

www.kwpub.in

Published in India by

Kalpana Shukla
KW Publishers Pvt Ltd
NEW DELHI: 4676/21, First Floor, Ansari Road, Daryaganj, New Delhi 110002
Phone: +91.11.23263498 / 43528107
email: mail@kwpub.in / knowledgeworld@vsnl.net
MUMBAI: 15 Jay Kay Industrial Estate, Linking Road Extn., Santacruz (W), Mumbai 400054
Phone: +91.22.26614110 / 26613505
email: mumbai@kwpub.in

Printed and Bound in India

Contents

1. Introduction 1

2. 'Informationisation' of Future Wars 3

3. Role of Information Warfare 7

4. Tactics of Information Operations 11

5. Cyber Warfare: New Age Strategy 16

6. 'Strategising' Space: Assessing Chinese Capabilities 20

7. Conclusion 30

‘Informationising’ Warfare: China Unleashes the Cyber and Space Domain

Introduction

In the age of globalisation, warfare now encompasses political, economic, diplomatic, cultural, and psychological dimensions, in addition to the earlier land, sea, air, space, and electronics spheres. As a result, the military sphere may no longer necessarily serve as the dominant sphere in present or future conflicts. On the contrary, there is increasing likelihood that future wars will be conducted in spheres not traditionally concerned with war. As a matter of fact, Lian Xiangru’s diplomatic battle of “returning the jade in an undamaged condition to Zhao” and the virtual war conducted by Mo Zi and Gongshu Ban, were classical examples of winning or precluding a war with non-military actions.[1]

According to “Warfare Beyond Rules: Judgment of War and Methods of War in the Era of Globalization,”[2] the central premise in Chinese military thinking is that if China ever has to defend itself, it should be prepared to conduct “warfare beyond all boundaries and limitations.” ‘Beyond military spheres’ include diplomatic, data network, intelligence, psychological, technological, smuggling, drug, simulated war, financial trade, resources, economic aid, legal, sanctions, media, and ideological war. Perhaps the most crucial among the ‘beyond rules’ criteria is manifested in the form of “asymmetric warfare”—for instance, guerrilla war (mostly urban), terrorist activities, and cyber attacks directed against data networks. The primary idea is to strike in unexpected ways against vulnerable targets.[3]

The era of the comprehensive use of highly developed technologies has been instrumental in providing greater room for applying wisdom and means towards military victory in the non-military spheres. While providing an account of China’s concept of *Unrestricted Warfare*, Qiao Liang

and Wang Xiangsui state, "If we want to have victory in future wars, we must be fully prepared intellectually for this scenario, that is, to be ready to carry out a war, which may be conducted in a sphere not dominated by military actions."[4] Qiao and Wang zero onto the most appropriate key, i.e., "unrestricted warfare." According to them, two coexisting ideas, i.e. "fight the fight that fits one's weapons" and "build the weapons to fit the fight", clearly demarcate traditional warfare from future wars and seek optimum tactics for the weapons one possesses.[5]

While outlining a war situation between two nations in possession of information technology and reliance upon traditional methods of operation, the attacking side would generally employ modes of greater depth, wide front, high strength and three-dimensionality, to launch a campaign assault against the enemy. Their methods do not go beyond satellite reconnaissance, electronic counter-measures, large-scale air attacks plus precision attacks, ground outflanking, amphibious landings, air drops behind enemy lines ... the result is not that the enemy nation proclaims defeat, but rather, one retaliates with one's own spears and feathers. Significantly, Qiao and Wang contend a 'combination scenario'. In such a scenario, the attacking side secretly musters large amounts of capital and launches a sneak attack on an adversary's financial markets. Subsequently, it inflicts a computer virus and hacker detachment in the opponent's computer systems and attacks his networks to disrupt and paralyse the networks of civilian electricity, traffic dispatch, financial transactions, telephone communications, and mass media, thereby causing social panic, street riots, and political crises for the adversary. Admittedly, these tactics do not attain the domain spoken of by Sun Tzu, namely, "The other army is subdued without fighting," but the force exercising the same can surely "subdue the other army through clever operations."[6]

Recommending psychological warfare forces for the future, Major General Xu Hezhen urged the Chinese leadership to:[7]

- Develop a psychological-warfare system that integrates specialised and non-specialised personnel, emphasising China's special characteristics;
- Establish a psychological-warfare coordination agency at the national level, to provide guidance and coordination for national psychological warfare actions;

- Establish a psychological-warfare command agency under the unified leadership of the Central Military Commission and the party committee;
- Establish several psychological-warfare scientific research agencies in order to guide both civilian and military work;
- Establish a specialised psychological-warfare corps that would form a consolidated and effective attack force;
- Develop a modernised basis for psychological-warfare material and technical equipment; and
- Form a psychological-warfare mentality by developing psychological warfare education for the masses and for all military commanders.

The aforementioned can be read as an inherently integrated part of the larger aim of China's foreign policy goals. While there is no official Chinese "grand strategy", the Chinese leadership appears to have reached a consensus over the objectives of the country's foreign policy and how to go about achieving them.[8] According to Avery Goldstein, China's grand strategy:

> ...aims to engineer China's rise to great power status within the constraints of a unipolar international system that the United States dominates. It is designed to sustain the conditions necessary for continuing China's program of economic and military modernisation as well as to minimise the risk that others, most importantly the peerless United States, will view the ongoing increase in China's capabilities, as an unacceptably dangerous threat that must be parried or perhaps even forestalled. China's grand strategy, in short, aims to increase the country's international clout without triggering a counterbalancing reaction.[9]

'Informationisation' of Future Wars

The Chinese military has been concentrating on developing a wide range of material and non-material capabilities that would make "defeating the superior with the inferior" possible.[10] The Chinese concept of "informationised warfare" could be interpreted as an outcome of transformation in the nation's mode of thinking. Traditional and mechanised methods of thought no longer seem to work in an integrated and systems-oriented environment, characterised rapidly by changing time-space relationships. As a result, the

strategic focus of the transformation remains "on changing the thinking style, introducing innovation in operational theory."[11]

In the opinion of the People's Liberation Army (PLA), these changes primarily focus upon transforming the military from a 'closed force' into a 'modern information-age power', focusing on new missions and roles. Not only is China's military reform process already underway, but Beijing is increasing its potential capability "to win local wars in the era of information"—as was highlighted in China's official 2008 *White Paper on National Defence*. While signifying the application of "informationised warfare" concepts to age-old Chinese military principles, that result in a new mode of thinking, PLA Major Peng Hongqi states:

> …treat the peacetime struggle for information supremacy as a 'genuine, perpetual, and never-ending battle' in preparations and implementation. It must practice strict information secrecy. The essence of information confrontation is to gain as much enemy information as possible and keep the enemy from gaining information on one's own side.[12]

Highlighting the requisite changes in the PLA's mode of thinking, Li Deyi, Deputy Chair of the Department of Warfare Theory and Strategic Research at the PLA's Academy of Military Science states:[13]

- Changing the mode of thinking is a requirement for ensuring victory in future wars. Group and organisational decision-making replaces individual thought;
- Strategy and technology are unified for planning purposes. The information superhighway can produce information misdirection, spread the 'fog of war', interfere with and disrupt the enemy's strategic perceptions. Electronic deception, camouflage, and interference, viral infiltration and interference with deception of satellites, can lead the enemy to make errors in judgment;
- Systems methodology has broken armies away from the singular cause and effect determinism that is characteristic of conventional warfare. Systems use information, information technology, and information system modes of thought to reduce an enemy's combat effectiveness;
- Information and information technology determines combat effectiveness, victory and defeat in war, and stand alongside materials and power as one of the three major strategic resources;

- Information deterrence (that is, information technology, weaponry, and resource deterrence as well as counter-information deterrence) are new modes of strategic thought and are important new deterrent forces, along with nuclear deterrence, in achieving national strategic objectives;
- New modes of thinking will enable breakthroughs in control theory;
- New modes of thinking integrate information reasoning, analysis, strategic capabilities, and the experiences of warfare, with information collection and storage, information processing, information transmission, and the logical reasoning capabilities of computers and artificial intelligence. The command, control, communications, computers, intelligence, information, surveillance, reconnaissance (C4I2SR) system decision-making is scientific, collective, real-time, and precise;
- Systemised warfare is represented by activities that have an organisational framework, planning, objectives, measures, layers and steps. It is networked thought built on a network foundation. Networks are systems—so systemisation thinking is also "networkisation" thinking, another new mode of thought; and
- The design of military system architectures, defensive alignments and attack counter-measures must utilise qualitative and quantitative analysis. Precise analysis, planning, design, guidance, and management are the requirements of the man/machine process for new thinking.

Resultantly, one of the transformations within the PLA since 2000 has been its effort to become an "informationised" force, that seeks to exploit advances in computers, communications, computer networks, long-range space and radar sensors and even information weapons to seek what the US refers to as "information dominance."[14] Richard D Fisher Jr. equates the PLA with the US military, where information warfare involving "soft-kill" and "hard-kill" options is concerned. The "soft-kill" options include using computer network attack, electronic warfare such as jamming, or electronic and high-power microwave devices to incapacitate military or civilian computer networks, weapons, or electronic equipment. The "hard-kill" options involve using anti-satellite weapons or anti-radiation missiles to destroy radar or communications nodes, or sending special forces to attack critical electronic targets.[15]

Senior Colonel Wang Baocun and Li Fei opine that the essential substance of information warfare, in the narrow sense, is made up of five core capabilities, which taken together, make for information operations (IO):[16]

- Substantive destruction: The use of hard weapons to destroy enemy headquarters, command posts and command and control (C2) centres;
- Electronic warfare: The use of electronic means of jamming or the use of anti-radiation (electromagnetic) weapons to attack enemy information and intelligence collection systems such as communications and radar;[17]
- Military deception: The use of operations such as tactical feints (simulated attacks) to shield or deceive enemy intelligence collection systems;
- Operational secrecy: The use of all means to maintain secrecy and keep the enemy from collecting intelligence on own operations; and
- Psychological-warfare: The use of TV, radio and leaflets to undermine the enemy military's morale.

As high technology is increasingly being incorporated into military functions, the boundaries between all five IO core capabilities are becoming further blurred.[18] Further, the two general areas include information protection (defence) and information attack (offence). The former aims at preserving one's own information systems and ensuring their operability, as these will become "combat priorities" – the key targets of enemy attack. The latter aims at disabling the enemy's combat command, control, coordination, intelligence and global information systems. Crucially, a successful information offence requires three prerequisites:[19]

- The capability to understand the enemy's information systems, and the establishment of a corresponding database system;
- Diverse and effective means of attack; and
- The capability to make battle damage assessments (BDA) of attacked targets.

The PLA has shifted the focus of informationisation from specific areas towards trans-area systems integration, as stated in the 2008 *White Paper on National Defence*. Aiming towards integration, the PLA is persisting in combining breakthroughs in key sectors with comprehensive development, technological innovation with structural reforms, and the development

of new systems, with the modification of existing ones to tap their full potential; enhancing systems integration; stepping up efforts to develop and utilise information resources; and gradually developing and improving the capability of combat based on information systems.[20] The PLA is placing high priority on command information systems. The integrated military information network came into operation in 2006, resulting in the further improvement of the information infrastructure, basic information support and information security assurance. Thereafter, progress has been made in the building of command and control (C2) systems for integrated joint operations, significantly enhancing the capability of battlefield information support. Besides, information technology (IT)-based training methods have undergone considerable development; surveying and mapping, navigation, weather forecasting, hydrological observation and space environment support systems have been further optimised; and a number of information systems for logistical and equipment support have been successfully developed and deployed; and full-scale efforts in building "digital campuses" have begun in PLA educational institutions.[21] The PLA, for palpable reasons, is focusing on information warfare (IW) in the narrow sense, as it primarily refers to wars in which information technology would be used to obtain or suppress information.[22]

Role of Information Warfare

"Information warfare is not just a theology," said Ming Zhou, adding that "they can integrate it into nation-state interests."[23] Crucial to any military's planning is the control of information critical to its consequent success. Communications networks and computers are of vital operational importance. The use of technology to accomplish both control and disruption of information flow has been referred to by several names, including information warfare, electronic warfare, cyber war, net war, and IO. Major General Wang Pufeng, widely recognised as the founder of Chinese IW, defined IW as:

> … a product of the information age, which to a great extent, utilises information technology and information ordnance in battle. It constitutes a "networkisation" (*wangluohua*) of the battlefield, and a new model for a

> complete contest of time and space. At its center is the fight to control the information battlefield, and thereby, to influence or decide victory or defeat.[24]

Outlining the major objectives of IW, James Mulvenon has succinctly stated, "The aim of IW in Chinese literature is information dominance (*zhixinxiquan)*."[25] Similar to the American concept of "information superiority", Chinese IW seeks to disrupt the enemy's decision-making process by interfering with the adversary's ability to obtain, process, transmit, and use information. The paralysis of the opponent's information system and decision-making cycle would, in turn, destroy the adversary's will to resist or fight on. Mulvenon argues that the Chinese obsession with IW as a preemptive weapon poses a volatile policy challenge:

> When one imagines scenarios in which the PLA would be concerned with preemptively striking US forces during the deployment phase for early strategic victory, it is difficult to avoid the obvious conclusion that the author (Lu Linzhi) is discussing a Taiwan conflict. For the PLA, using IW against US information systems to degrade or even delay a deployment of forces to Taiwan, offers an attractive asymmetric strategy. American forces are highly information-dependent and rely heavily on precisely coordinated logistics networks… if PLA information operators using PCs were able to hack or crash these systems, thereby delaying the arrival of a US carrier battle group to the theater, while simultaneously carrying out a coordinated campaign of short-range ballistic missile attacks, "fifth column," and IW attacks against Taiwanese critical infrastructure, then Taipei might be quickly brought to its knees and forced to capitulate to Beijing.[26]

In a description of IW as a new form of People's War, Wei Jincheng opined that the technological revolution provided only a stage for confrontations. It was only when this revolution was married with military operations could it take on the characteristics of confrontation. Wei further stresses upon the integrity of the information systems and underlines the multi-dimensional, interconnected networks on the ground, in the air (or outer space) and under water, as well as terminals, modems and software, as not only instruments,

but also weapons. A People's War under such conditions, according to Wei, would be complicated, broad-spectrum and changeable, with high degrees of uncertainty and probability, which would require full preparation and circumspect organisation.[27]

In fact, General Gordon R Sullivan, former Chief of Staff of the US Army, maintained that information warfare would be the basic form of war-fighting in future warfare, thus advocating the concept of precision warfare (dubbed as 'non-contact attack' by the US), based on the perception that "there will be an overall swing towards information processing and stealthy long-range attacks as the main foundations of future warfare."[28] In 2002, the PLA's IW General Staff proponent, General Dai Qingmin, listed six forms of IW in *China Military Science,* which encompassed operational security, deception, computer network attacks, electronic warfare, intelligence, and physical destruction. Dai also analysed China's concept of "integrated network-electronic warfare (INEW)" similar to the US concept of network-centric warfare. The concept refers to a series of combat operation actions with the integrated use of electronic warfare (EW) and computer network warfare (CNW) measures on the informationised battlefield. The actions are designed to disrupt the normal operations of the enemy's battlefield network information systems and protect one's own. According to Dai, the objective of INEW is to seize battlefield information superiority.[29]

It has been established by the aforementioned arguments that IW is playing a serious role in the transformation of the PLA from a mechanised to an informationised force. An instance of this transition was in evidence when on 06 August 2003, Defence Minister Cao Gangchuan addressed a meeting of municipal government personnel, the PLA General Staff, and the Beijing Military Region staff, stressing that the PLA's defence build-up was aimed at gaining victory in IW—with the IW-directed effort receiving the complete support of the Central Military Commission (CMC).[30] In nearly every training exercise, a "blue (IW-based) army" has superiority in technology, which forces a "red (IW-deficient) army" to rely on back-up systems or the employments of counter-tactics, which might indicate that the PLA expects to absorb a first IW strike.[31] Besides, other more specific issues which stand out in the open-source analysis of IW, IO, and IS theory, and would probably carry over into the next ten years of the PLA's development, are:

- Joint offensive IW is considered an important aspect for attainment of victory in the information age by the Chinese leadership.
- Psychological-warfare shall assume an elevated role in future wars.

To demonstrate the emphasis on offensive IW, one needs look no further than the militia. For instance, for the past few years, the Guangzhou city militia was focused on the requirements of the information battlefield. It was decided to organise a battalion headquarters (set up as a provincial telecommunications company and an electronic warfare company). The computer network company possesses two platoons, a network defence platoon and a network attack platoon; the electronic warfare company has two platoons, one devoted to reconnaissance and the other to deception. Significantly, a draft "Training Plan for Militia Information Technology Elements" was developed from discussions with staffs of the Guangzhou Military Region (MR). The training research in 2003 was inclusive of protecting one's own network security, searching for enemy network stations, and attacking enemy networks.[32]

In March 2003, military representatives attending the National People's Congress (NPC) noted that IW units had "already developed electronic jamming/bombardment weapons" capable of paralysing all enemy electronic systems, including the Internet and military command systems. Several trial units were established, and a large portion of the budget was directed towards the advanced development of IW units. On 04 November 2003, President Jiang Zemin urged the armed forces to build IW units in order to win in IW and emphasised, "New types of soldiers with new military theories are needed to do this."[33] Additionally, the PLA intends to establish a command structure for psychological warfare as well as create special units that would attempt to overcome traditional Chinese inferiority in high-tech weapon systems.[34]

Since bypassing major mechanised-age stumbling blocks, both China and Russia have learnt from the mistakes committed by others and have become IW forces to reckon with.[35] As the Chinese say, "Borrow a ladder to climb the tree"—aptly describing the lessons that China has learnt at the cost of others. Describing the high stakes involving IW, Timothy L Thomas opines that the Chinese believe that losers in IW will not just be those with backward technology; but also those who lack command thinking and the ability to apply

strategies. Success in IW could lead China to play an important strategic deterrent role in the Asia-Pacific region in the future. Surely, Beijing sees a strategic opportunity to leapfrog the age of mechanisation and graduate directly into the age of information.[36]

Tactics of Information Operations

Acknowledging the significance of information operations, Peng Guangqian and Yao Youzhi, state in their account, *The Science of Military Strategy,* that a small-scale tactical information operation can achieve strategic or operational purposes; therefore, the operational limits of traditional strategic, operational and tactical levels are increasingly getting blurred.[37] The use of cyberised weapons allows information operations to break through the boundaries of the traditional battlespace. The depth, front and altitude of the battlefield of information operations are expanded and at the same time, the force density is reduced.[38] Accepting the premise that the belligerent in a future war shall contend for information superiority, Dai Qingmin maintained that information control was essential in order to create conditions for maintaining the initiative and winning final victory.[39]

According to the US Department of Defence's Annual Report (2004) to Congress on the *Military Power of the People's Republic of China*, the Chinese military was believed to be enhancing its information operations capabilities by placing specific emphasis on the ability to perform information operations, designed to weaken an enemy force's command and control (C2) systems.[40] There is no ambiguity in the manner in which the Chinese view information operations:[41]

- Intelligence operations, which include intelligence reconnaissance and protection;
- C2 operations to disrupt enemy information flow and weaken its C2 capability while protecting one's own;
- Electronic warfare, by seizing the electromagnetic initiative through electronic attacks, electronic protection and electronic warfare support;
- Targeting enemy computer systems and networks to damage and destroy critical machines and networks and the data stored on them; and
- Physical destruction of enemy information infrastructure such as C4I2SR through the application of firepower.

Additionally, the Pentagon's 2007 report on the PLA's computer network operations provided valuable insight into the PLA's capabilities, as far as seizing the initiative towards electromagnetic dominance in the event of a conflict is concerned:

> China's computer network operations (CNO) include computer network attacks, computer network defense, and computer network exploitation. The PLA sees CNO as critical to seize the initiative and achieve "electromagnetic dominance" early in a conflict, and as a force multiplier. Although there is no evidence of a formal Chinese CNO doctrine, PLA theorists have coined the term "Integrated Network Electronic Warfare" to outline the integrated use of electronic warfare, CNO and limited kinetic strikes against key C4 nodes to disrupt the enemy's battlefield network information systems. The PLA has established information warfare units to develop viruses to attack enemy computer systems and networks, and tactics and measures to protect friendly computer systems and networks. The PLA has increased the role of CNO in its military exercises. For example, exercises in 2005 began to incorporate offensive operations, primarily in first strikes against enemy networks.[42]

Strategic information operations should establish the dictum of 'giving priority to attack and combining attack with defence'. Launching preemptive attacks to gain battlefield initiative and simultaneously launching information attacks actively is the key to seizing information superiority and battlefield initiative. Owing to the characteristics of information technology, the one whose information technology develops faster, relies more on information systems. By launching active information attacks, striking the enemy's information centre of gravity and weakening the combat efficiency of its information systems and cyberised weapons, one can crucially weaken its information superiority and consequently, reduce combat efficiency.[43]

Only by conducting comprehensive information defensive operations and ensuring that one's own information systems and cyberised weapons remain impervious, can one reduce the efficiency of the enemy's information attacks, better organise one's own information attacks and create favourable conditions for information operations. But defensive operations can neither directly threaten the enemy's information systems nor greatly weaken its

information superiority. Only information attacks can directly disturb and destroy the enemy's information systems, and, therefore, weaken its combat efficiency significantly—a principle that China is seen to be mastering.[44]

It would be crucial to mention here that Chinese analysts have outlined and absorbed the four main forms of war-fighting that are likely to take place in the future according to the US: (1) information warfare; (2) precision warfare;[45] (3) joint operations; and (4) military operations other than war (MOOTW).[46] According to the 2008 *White Paper on National Defence*, China is focusing on training its armed forces for MOOTW, including UN peacekeeping and peace support operations, anti-piracy missions, counter-terrorism, environmental disasters and social/civil unrest. Beijing regards MOOTW as an imperative tool for projecting national power and is scientifically devising plans for the development of MOOTW capabilities. The PLA has intensified strategic and operational-level command post training and troop training in conditions of informationisation, holding trans-regional evaluation exercises, conducting whole-unit night training and carrying out integrated exercises for logistical and equipment support. These efforts provide evidence of China's gradual move towards employing its armed forces as an instrument of statecraft, to achieve major national security objectives and to display the Chinese flag as well as mark Chinese presence around the world.[47]

It is widely noted that Chinese military analysts consider "control" to be nearly as important as information superiority. Again, the former results in the latter. China's focus for attaining information superiority/control is built around the use of stratagems, whereas the US focuses on speed and efficiency. China views network-centric operations in a slightly different manner from the US, calling their nearly equivalent theory "integrated network-electronic warfare" or as one Chinese expert explained it, the "informationisation of warfare."[48]

A commentary in the *People's Liberation Army Daily* in 2003 underlined the need for China to protect its "information territory", giving an indication of what it might consider targeting in foreign countries. According to this definition, information territory "not only refers to the Internet in [the] common sense, but also to key information network systems such as finance, electric power, telecommunications, transportation, energy, military and statistics."[49]

It became apparent by 2004 that six of the seven Military Regions (MRs) would possess a "Special Technical Reconnaissance Unit" (STRU) intended to wage both defensive and offensive information warfare. As such, it is reasonable to envision that between the STRU and less formal reserve and militia units, the PLA could maintain a force of thousands of "cyber warriors". Only the Beijing MR lacked such a unit, but that could be attributed to the fact that Beijing served as the command headquarters for the PLA.[50] At the strategic level, defence analysts view information operations and computer network operations as useful supplements to conventional war-fighting capability, and powerful asymmetric options for "overcoming the superior with the inferior." According to a People's Republic of China (PRC) author, "computer network attack is one of the most effective means for a weak military to fight a strong one."[51] Therefore, at an operational level, the emerging Chinese IO strategy displays the following key features:[52]

- China emphasises defence as the top priority, with the belief that the US is already carrying out extensive computer network exploit activities against Chinese servers;
- IW is viewed as an unconventional warfare weapon, to be used in the opening phase of the conflict, not a battlefield force multiplier that can be employed during every phase of the war;
- IW is seen as a tool to permit China to fight and win an information campaign, precluding the need for conventional military action;
- China comprehends that the US is "information dependent", while Beijing is not. However, the latter is a misperception, given that the current Chinese C4I2 modernisation is, paradoxically, making China more vulnerable to US methods;
- Computer network attacks are characterised as a preemption weapon to be used under the rubric of the rising Chinese strategy of *xianfa zhiren*, or "gaining mastery before the enemy has struck".

Computer network attacks appear particularly attractive to the PLA, since they have a longer range than its conventional power projection assets. This endows the PLA with the ability to "reach out and touch" the US. Yet, a computer network attack is also believed to enjoy a high degree of "plausible deniability", rendering it a possible tool of strategic

denial and deception.[53] It is important to note that the Chinese computer network attack (CNA) doctrine focuses on disruption and paralysis and not destruction. Philosophically and historically, the evolving doctrine draws inspiration from Mao Zedong's theory of "protracted war", in which he argued, "We must, as far as possible, seal up the enemies' eyes and ears, and make them become blind and deaf, and we must, as far as possible, confuse the minds of their commanders and turn them into madmen, using this to achieve our own victory."[54] In the modem age, it is asserted, "computer warfare targets computers—the core of weapons systems and C4I2 systems in order to paralyse the enemy". The goal of this paralysing attack is to inflict a "mortal blow" (*zhiming daji*), though this does not necessarily refer to defeat. Instead, Chinese analysts often speak of using these attacks to deter the enemy, or to raise the costs of conflict to an unacceptable level. Specifically, computer network attacks on non-military targets are designed to "... shake war resoluteness, destroy war potential and win the upper hand in war," thus, undermining the political will of the population for participation in military conflict.[55]

Timothy L Thomas further highlights the following information attack options that have been outlined by diverse PLA sources: planting information mines; conducting information reconnaissance; changing network data; releasing information bombs; dumping information garbage; applying information deception; releasing clone information; organising information defence; and establishing network spy stations.[56]

The PLA was reported to have operational computer-warfare units in the Guangzhou, Nanjing and Jinan MRs, each with about 500 specialists in 2001.[57] Yet another 2001 report indicated that PLA information warfare reserve units were established in the cities of Datong, Xiamen, Shanghai, Echeng and Xian. It is plausible that such reserve units include specialists who work in the civilian computer development and manufacturing sector.[58] Within the PLA, the Shijiazhuang Army Command College, the Navy Command Academy, the Air Force Command Academy and the Second Artillery Corps Command Academy met in July 2003 to work out an overall joint teaching programme for the three armed forces to share information resources and exchange experiences via the Internet.[59]

Cyber Warfare: New Age Strategy

Cyber warfare is a brand new operational pattern that has emerged and developed in the context of global cyberisation. According to Peng Guangqian and Yao Youzhi, cyber warfare uses advanced information technologies to disintegrate, damage or destroy key computer systems and computer networks as well as information stored in them.[60] They further illustrate that cyber warfare consists of two types: cyber attacks and cyber protection. Cyber attacks include virus attacks and hacker attacks. Computer virus attacks refer to operational actions that use computer viruses to destroy or tamper information stored in computer systems, such that they do not work properly. In the military field, the core equipment of military information systems and cyberised weapons are all likely targets of computer virus attacks. Computer hacker attacks refer to those actions taken by hackers to intrude upon and destroy an opponent's cyber systems.[61]

In 2008 and earlier, computer systems around the world, including those owned by the US government, continued to be targets of intrusions appearing to have originated from China. Notwithstanding that these intrusions focused on exfiltrating information, the access and skill required for intrusions are similar to those necessary to conduct computer network attacks. However, it remains ambiguous if these intrusions were conducted by, or with the endorsement of, the PLA or other elements of the Chinese government. Nevertheless, it is a well-accepted fact that developing capabilities for cyber warfare is consistent with PLA military writings on the subject, which could best be termed as commandingly authoritative.

In a statement to the US Congress in March 2007, General James E Cartwright, Chief of the US Strategic Command, accepted that "America is under widespread attack in cyberspace." During the 2007 fiscal year, the Department of Homeland Security received 37,000 reports of attempted breaches on government and private systems, which included 12,986 direct assaults on federal agencies and more than 80,000 attempted attacks on Department of Defence computer network systems. In fact, some of these attacks are believed to have "reduced the US military's operational capabilities."[62] As for China's part in this trend, one American cyber security firm, that focuses on a centralised group of activity based from China, stated, "In the last three months, the attacks [from China] have almost tripled."[63]

Besides, in December 2007, the *New York Times* reported that in a series of "sophisticated attempts" against the US nuclear weapons lab at Oak Ridge, Tennessee, Chinese hackers had been able to "remove data."[64] The report highlighted an alarming fact—China's cyber spies were now a part of America's computer networks, along with other countries, crucially including India.

By far, the target attacked most intensely by the Chinese is the US military, closely followed by the State Department, the Commerce Department, and the Department of Homeland Security. In a key statement, a US cyber security expert confessed to a group of federal managers, "The Chinese are in half of your agencies' systems already."[65] Cyber warfare units in the PLA are said to have already penetrated the Pentagon's unclassified but sensitive Nonsecure Internet Protocol Router Network (NIPRNet) and have designed software to disable it in times of conflict or confrontation.[66] Major General William Lord, Director of Information, Services and Integration in the Air Force's Office of Warfighting Integration, admitted, "China has downloaded 10 to 20 terabytes of data from the NIPRNet already… there is a nation-state threat by the Chinese."[67]

Richard Lawless, Deputy Under Secretary of Defence for Asia-Pacific Affairs, testified to a Congressional panel on 13 June 2007, that the Chinese were "leveraging information technology expertise available in China's booming economy to make significant strides in cyber-warfare." He further noted that the Chinese military's "determination to familiarise themselves and dominate, to some degree, the Internet capabilities—not only of China and that region of the world—provide them with a growing and very impressive capability that we are very mindful of and are spending a lot of time watching."[68] Lawless testified:

> The Chinese have developed a very sophisticated, broadly based capability to... attack and degrade our computer systems and our Internet systems. Computer access, warfare and the... disruptive things that allows you to do to an opponent are well appreciated by the Chinese and they spend a lot of time figuring out how to disrupt our networks—how to both penetrate networks in terms of gleaning or gaining information that is protected, as well as computer network attack programs which would allow them to shut

> down critical systems at times of emergency. So, first of all, the capability is there. They're growing this capability as they see it as a major component of their asymmetric warfare capability.[69]

As far as the macro-level targets are concerned, the Chinese have identified two specific computer network operations: military network information and military information stored on networks. Computer network attacks seek to use the former to degrade the latter. Chinese CNA targeting, therefore, focuses specifically on "enemy C2 centers", especially "enemy information systems". Of these information systems, PLA writings and interviews suggest that logistics computer systems have emerged as a top military target. According to one PLA source, "We must zero in on the...crucial links in the system that moves enemy troops... such as information systems." Another source states, "We must attack system information accuracy, timeliness of information, and reliability of information."[70]

It should be recalled that in August 1999, following the conclusion of the cross-strait hacker skirmish that erupted in the wake of Taiwanese President Li Teng-hui's declaration that the island's relationship to the mainland was a "state-to-state relationship", a *Liberation Army Daily* article lauded the "patriotic hackers" and encouraged other hackers to join in during the next crisis with Taiwan.[71] Nevertheless, even if the Pentagon does not directly accuse the Chinese military or government of the attacks, it asserts that the incidents are consistent with the current military thinking that has evolved in China. David Sedney, Deputy Assistant Secretary of Defence for East Asia, United States Department of Defence, identified cyber-warfare as an area of growing concern and called on the Chinese to clarify their intentions as, "The techniques that are meant for these intrusions are certainly consistent with what you would need if you were going to actually carry out cyber-warfare… consistent with a lot of writings we see from the Chinese military and Chinese military theorists." As Chinese cyber warfare advances, coupled with China's increasing skill at neutralising information-transmitting satellites and other capabilities—it fulfills a part of its military objective of crippling potential foes, in the event of its crisis or confrontation.[72]

In what have widely been viewed as efforts to coordinate the defence of Pentagon computer networks and improve offensive capabilities in cyber

warfare, the US military has set up a new 'cyberspace command', as announced by the Pentagon on 23 June 2009, when Robert Gates, the US Secretary of Defence, authorised the development of offensive cyber-weapons and defence of command and control networks of the US armed forces against computer attacks. This is the first such formation that would operate under the US Strategic Command. Reported breaches of the US electricity grid and of networks used by aerospace contractors building the F-35 fighter jet have further highlighted concerns over cyber security. Washington has long stressed that China has built up a sophisticated cyber warfare programme and that a spate of intrusions in the US and elsewhere can be traced back to Chinese sources. US authorities are still investigating whether PRC officials secretly copied contents of a US government laptop during a visit to China by the US Commerce Secretary in May 2008 and used the information to try to penetrate into US Department of Commerce computers.

The low cost of entry (for example, a laptop connected to the Internet), and the ability to operate anonymously, are factors that makes cyberspace attractive to nations such as China, who realise that challenging a technologically superior nation like the US in a symmetrical contest would prove be a daunting task. According to Brigadier Gurmeet Kanwal (Retd), "The information warfare has gradually assumed the position to be regarded as an extremely attractive option in China, since they view it as an asymmetric tool that would enable them to overcome their relative backwardness in military hardware."[73] Needless to say, this appears to have become a key driver so as to develop capabilities to attack or degrade US civilian and military networks.[74]

China has been openly engaging in cyber war against the US and India on a regular basis. In May 2008, Chinese hackers allegedly broke into the Indian Ministry of External Affairs' internal communication network.[75] Subsequently, the Belgian government warned that e-mail attacks, aimed at compromising government computers, appeared to be coming from China.[76] In March 2009, former Indian Foreign Secretary Shivshankar Menon, admitted that there had been attempts at hacking into the computers of Indian embassies, in response to media reports of a vast cyber network controlled from China, that targeted governments and private computers in 103 countries, including those of the Indian embassy in Washington.[77] There were reports

in leading regional newspapers in India in December 2009 regarding secret and sensitive documents being hacked from the Corps Headquarters of the Indian Army's Eastern Sector formations. The computer networks in these areas had been infected by Chinese Trojan attacks often. In another five to 10 years, China will have developed much greater depth and sophistication in its understanding and handling of IW techniques and information operations. With Indian society becoming increasingly dependent on automated data processing and vast computer networks, India will also become extremely vulnerable to such IW techniques. The fact that it can be practised from virtually any place on the earth, even during peace-time, makes paralysis warfare even more diabolical. India can ill-afford to ignore this new challenge to its security.[78]

Open-source studies in China make it thoroughly evident that reserves, militia, PLA, and the civilian forces would most likely conduct joint IW operations in the future and join hands against any intervening IW force. This integration is already underway, as signified by the proposed establishment of a cyber security force. Significantly, Qu Yanwen, a security specialist, has proposed a Cyber Security Force (CSF), constituting members of the PLA, the Ministry of State Security and Public Security, and technical specialists.[79]

As the PLA has transitioned from the operational concept of "Joint Operations" to "Integrated Joint Operations", it has also greatly enhanced its ability to conduct network-based military activities. In early 2000, it was reported that the PLA was building a new integrated C41SR system called "Qu Dian".[80] Also referred to as the Regional Integrated Electronic System, or Project 995, this new C4IKSR (China adds 'K' for kill) system builds on several years of PRC investments in building fibre-optic networks. It consists of cellular and satellite communication networks throughout the PRC, integrated with new satellite, aircraft and electronic sensors. It is believed to consist of a Joint Operations Centre that is linked to joint command centres in the Nanjing, Guangzhou and Jinan MRs as well as to Navy, Air Force and Second Artillery Commands in these MRs.[81]

'Strategising' Space: Assessing Chinese Capabilities

Information superiority is seen by the PLA as a primary component for winning future wars.[82] There is a growing sense of assertion within and

outside the ranks of the PLA, including among Chinese analysts, that the control of space is a prerequisite for control of the terrestrial domains.[83] According to one source:

> Space power improves battlefield awareness capabilities, strengthens joint operations systems, improves precision strike capabilities, and increasingly strengthens overall battlefield superiority. Integrated joint operations increasingly rely on space power and space is the high point of informationised warfare.[84]

Augmentation of China's space and counter-space capabilities provides a mirror that reflects upon the rise of Chinese power. Treating space as another domain of the global commons, in which warfare is permitted, goads Larry M Wortzel to argue that China has conceptualised it as the ultimate high ground, which must be dominated in order to secure favourable political outcomes terrestrially.[85]

China's space programme represents a major investment, aimed at enabling Beijing to utilise space in expanding its national power. The advancements in space technologies have become critical to the successful conduct of military operations as they enable Beijing to use its armed forces more effectively, either because they permit better collection, transmittal and exploitation of information or because they support the development of new weapons such as responsive directed energy and other non-kinetic technologies. China's space policy goals could be characterised as simultaneously focused on securing economic and development benefits, enhancing national military capabilities, and procuring symbolic benefits that both aid regime survival at home and enhance Chinese prestige abroad.[86]

Although a now-civilianised Commission on Science, Technology, and Industry for National Defence (COSTIND) sits at the apex of the Chinese defence-industrial complex, it is responsive to both the Central Military Commission of the Chinese Communist Party (CCP) and the General Armaments Department of the PLA. According to Kevin Pollpeter, "China's space programme is inherently military in nature…indeed, it is a military-civilian joint venture in which the military develops and operates its satellites and runs its infrastructure, including China's launch sites and satellite

operations center."[87] This principally puts forth that the civilian aspects of China's space programme ultimately ends up serving its military arm. Ashley J Tellis further argues that China's space achievements mask important weaknesses in technological sophistication, gaps in capability, and operating regimes, thus, compelling it to look for foreign technology—bought, copied, stolen or acquired through joint ventures—as solutions designed to overcome its weaknesses.[88]

China's space launch capability is centred on ten different Long March booster configurations, capable of deploying various payloads from low-earth to geosynchronous orbits. These launch vehicles primarily use three launch sites: recoverable satellites and manned spacecraft, launched from the Jiquan Satellite Launch Centre in Gansu Province; orbital platforms headed for geostationary orbit, launched from Xichang Satellite Launch Centre in Sichuan Province; and satellites intended for polar orbit, launched from the Taiyuan Satellite Launch Centre in Shanxi Province. China also intends to construct a new spaceport on Hainan Island, which would be optimal for launches aimed at equatorial orbits, but it remains unclear when this facility would become operational. Owing to the fact that fixed launch sites are inherently vulnerable, the Chinese demonstration of a mobile launch capacity, exemplified by the Pioneer rocket, represents a significant innovation, insofar as it would bestow on Beijing a responsive launch capability, even if its fixed bases were destroyed.[89]

China has launched scores of satellites since its first launch in 1970, though the exact number currently operational remains unclear. Nevertheless, what is certain is that the satellites associated with its military-civil programme are quite diverse. The largest number of satellites and perhaps the most impressive capability seems to reside in China's communications platforms: these include satellites in the Chinasat, APStar, Asiasat, and Sinosat series, which are either owned by China or are privately owned regional systems that lease transponders to Chinese users.[90] Beijing also utilises foreign satellite systems such as Intelsat and Inmarsat and operates a series of Earth surveillance satellites, capable of providing imagery intelligence, remote sensing data, oceanographic information, synthetic aperture radar (SAR) imagery, and environmental monitoring: the Ziyuan, China Brazil Earth Resources Satellite (CBERS-2), Haiyang 1, JianBing 5, and Huanjing series

respectively, represent examples of such capability. Besides, China has also achieved crucial access to Landsat data and uses foreign commercial satellite products extensively for military intelligence purposes.[91]

China's satellite capabilities suggest that its indigenous systems, combined with its access to foreign platforms or services, provide its military forces with sufficient capability as far as communications, remote sensing/reconnaissance, navigation, and meteorological services are concerned, within China's borders or at some distance around them. The new signals intelligence (SIGINT)/ electronics intelligence (ELINT) platforms, electro-optical and SAR imagery satellites, and dedicated data relay satellites likely to be launched within the next decade, would enable the PLA to expand its battlespace awareness and targeting capabilities tremendously, support its regional presence and projection operations in East and Southeast Asia and in the Indian Ocean, and fill the missing links required to complete its area and access denial strategy vis-à-vis the United States across the entire western Pacific.[92]

Besides the Chang'e-1 lunar probe, which was launched in late 2007, the second lunar orbiter, Chang'e-2 is scheduled to be launched in 2010. China is also planning for the launch of a landing craft and rover on the moon called Chang'e-3, in 2013. Significantly, China has begun the development and testing of the Long March V rocket—the world's largest. This is planned to be operational by 2015. Intended to lift heavy payloads into space, it will more than double the sizes of low earth orbit (LEO) and geosynchronous earth orbit (GEO) payloads that China can place into orbit. To support these new rockets, the construction of a new launch facility near Wenchang on Hainan Island began in 2008. The Chinese leadership continues to remain silent and maintains considerable opacity about the military applications of its space programmes and counter-space activities.[93]

According to Bao Shixiu, a Chinese military scholar at the PLA Academy of Military Science:

> An effective active defence against a formidable power in space may require China to have an asymmetric capability against the powerful United States. Some have wondered whether a defensive policy applied to space suggests that China's possession of a robust reconnaissance, tracking, and monitoring space system would be sufficient for China to prevent an attack in space and

> would be in line with China's 'doctrinal' position of 'defensive' capabilities. In essence, China will follow the same principles for space militarisation and space weapons as it did with nuclear weapons. That is, it will develop anti-satellite and space weapons capable of effectively taking out an enemy's space system, in order to constitute a reliable and credible defense strategy.[94]

Since these goals are critical to China as a rising power in the larger global context, Beijing cannot be expected to trade away its counter-space capabilities for an arms-control regime that would further accentuate its competitors' military advantages.[95]

In a testimony before the Senate Armed Services Committee, General James E Cartwright, Chief of the US Strategic Command, declared:

> The Chinese have undertaken what we would call a very disciplined and comprehensive continuum of capability against our space capabilities. These efforts range all the way from [achieving] temporary and reversible effects to permanent damage exacted through direct ascent ASAT … [and] eventually … co-orbital [weapons], which thereby demonstrates … that they have a very comprehensive [vision for] what they want to be able to do as a nation in their region.[96]

For more than a decade, Chinese military strategists and aerospace scientists have been constructing a blueprint for achieving space dominance.[97] The Chinese vision of space warfare involves not just denying space to its adversaries but using space for affirmative ends such as the intercept of ballistic and cruise missiles through space-based combat platforms; strikes by space systems on terrestrial targets; and attacks by land, air, sea, aerospace and space vehicles on an adversary's space platforms and space-based command and control assets and their associated terrestrial nodes.[98] As Senior Colonel Yao Yunzhu stated, "... My prediction: outer space is going to be weaponised in our lifetime."[99] Consistent with these expectations, Chinese military writings emphasise the need for dedicated space forces and advanced space weapons and support capabilities, designed to prosecute the full spectrum of 'space safeguard,' 'space support' and 'space attack' operations.[100]

Beijing has been pursuing a diverse and comprehensive portfolio of space warfare investments since the late 1980s. The status of these programmes runs from advanced concept development and testing, through product engineering evaluation, line-level manufacturing and acquisition from foreign sources, to integration as war-fighting capabilities into the Chinese armed forces. The evidence suggests that these programmes are protean: they lend themselves to steady evolution across the spectrum, from space denial to space dominance, if Beijing's political goals change over time, though at present and for the foreseeable future, they are optimised for the space-denial mission.[101]

Given the importance of space awareness for military operations, Chinese planners have been developing and maintaining an increasingly comprehensive catalogue of relevant space objects.[102] As a matter of fact, the US Department of Defence declared as early as 2002, "China probably has a thorough knowledge of US and foreign space operations, based, in part, on access to open-source information on US space systems and space operations."[103]

Further, according to the Pentagon's 2009 *Annual Report to the Congress*, China is rapidly improving its space-based intelligence, surveillance, reconnaissance, navigation, and communications capabilities, allowing for greater military support from space. Concurrently, China is also developing a multi-dimensional programme to improve its capabilities to limit or prevent the use of space-based assets by potential adversaries, during times of crisis or conflict. Although China's commercial space programme has utility for non-military research, it demonstrates space launch and control capabilities that have direct military applications. China conducted as many as 11 space launches in 2008, putting 15 satellites in orbit. Included in this number are four new remote sensing satellites: Yaogan-4, Yaogan-5, Huanjing-1A, and Huanjing-1B; the Shenzhou-VII manned spacecraft, along with its accompanying small satellite, Banxing-1; three communications satellites; and, two meteorological satellites. In April 2008, China successfully launched its first data relay satellite— TianLian-1. According to PRC news broadcasts, TianLian-1 was initially tasked to support the launch of Shenzhou-VII manned space mission, increasing surveillance and control coverage of the manned spacecraft's path from 12 percent to roughly 60 percent.[104]

In the view of PLA defence experts, "Whoever has control (or 'hegemony') over space, will also have the ability to help or hinder and affect 'ground' mobility and air, sea and space combat."[105] And while calling for the "peace-loving nations and peoples of the world to oppose the weaponisation of space," the PLA continued to "heed the call of Communist Party Central Military Commission Chairman Jiang Zemin for China to become a strong military technologically."[106]

The emergence of potent Chinese counter-space capabilities makes US military operations in Asia more risky than ever. The threat has not arisen due to a lack of a space arms-control regime, or because of the Bush Administration's disinclination to negotiate an accord that bans the weaponisation of space. Rather, it is rooted entirely in China's requirement that it should be able to defeat the United States in a regional conflict despite its conventional inferiority. This strategic challenge has compelled Beijing to exploit every anti-access and battlespace-denial technology potentially available.[107]

China's military space capabilities are currently manifested in five distinct areas: (i) space launch capabilities; (ii) the telemetry, tracking and command (TT&C) network; (iii) space orbital systems; (iv) connectivity to military operations; and (v) counter-space technologies. China's military space capabilities cannot be understood outside the context of its military strategy, which today is summarised by the phrase "active defence". David Finkelstein states that this approach remains oriented towards defence at the strategic level. Beijing's current military strategic guidelines require the PLA to prepare for such an active defence in a specific context, namely what could now be termed "conditions of informationisation."[108]

According to Ashley J Tellis, space has acquired a privileged position, where Chinese military thinking appears to be gravitating towards three broad conclusions. Firstly, China must develop the entire spectrum of capabilities required to exploit space in the manner necessary to advantage its conventional military operations against a wide range of potential adversaries. Secondly, China must prepare to deny space to superior adversaries, who could otherwise use their vulnerable but sophisticated space systems to multiply the conventional military advantages they already enjoy vis-à-vis Beijing. And thirdly, the centrality of space to information dominance and

the pivotal significance of information dominance for producing victory in war imply that a struggle for space control is inevitable and, consequently, China must prepare itself for such rivalry by fully integrating space into its own military operations and, as required, developing its own space-related deterrent and war-fighting capabilities.[109]

China is known to possess space-based ELINT or SIGINT capabilities, though the specific platforms associated with these missions are not identified. China does possess a space-based meteorological and weather assessment capability provided through its Fengyun series satellites and it has reception centres to receive foreign meteorological data.[110] It has now moved ambitiously into the navigation and positioning segment through its Beidou satellite constellation which, though not as precise as the US Global Positioning System (GPS), could nonetheless be used to improve the accuracy of China's conventional weapons.[111] Chinese capabilities in the realm of agile micro- and nano- satellites indicate that they can be launched quickly by small mobile boosters, or covertly as secondary payloads on large boosters, committed to what are otherwise peaceful space missions. Once in orbit, micro- and nano-satellites are extremely difficult to detect and track, lending them splendidly to co-orbital anti-satellite missions.[112] Chinese military planners have concentrated on electronic attack methods to stymie space assets, especially those of the US, located in medium earth, geosynchronous and eccentric orbits, where these other technologies are less effective. The most important targets are the tactical communications platforms in geosynchronous orbit and the GPS constellation in medium earth orbit.[113]

From an offensive standpoint, China is developing its own weapons. The PLA is experimenting with directed energy weapons that can destroy satellites and in theoretical research, is considering particle beam weapons that can engage missiles in flight.[114] The Chinese military reportedly is also considering the use of "piggy-back satellites" and "micro-satellites" that can be used as kinetic energy weapons, to destroy enemy satellites or spacecraft, or can attach themselves to enemy satellites to jam them.[115]

China has made enormous investments in developing counter-space capabilities. Its counter-space programmes today are remarkable for their diversity, depth and comprehensiveness, since they include major investments in:

- Upgrading China's space object surveillance and identification systems;
- Developing direct attack weapons to include direct ascent and co-orbital capabilities;
- Exploring directed energy weapons for dazzling or damaging orbiting satellites;
- Acquiring various technologies for electronic attack against space platforms and their associated links, as well as against conventional forces and their war-fighting operations; and
- Improving kinetic and non-kinetic forms of ground attack aimed at the control segments of an adversary's space infrastructure.

These counter space programmes continue to persist even after China's anti-satellite (ASAT) test in January 2007—an event that demonstrated, if nothing else, that all satellites traversing the Chinese mainland in low earth orbit are at risk.[116]

China's ASAT Potential

On 11 January 2007, a Chinese medium-range ballistic missile lifted off from a launch site at the Xichang space facility in Sichuan Province and slammed, several minutes later, into an ageing Chinese weather satellite, Fengyun-1C (FY-1C), deployed in LEO at an altitude of some 864 km.[117] According to Geoffery Forden, an analyst at the Massachusetts Institute of Technology, "The payload used to intercept the FY-1C could be used to destroy geostationary satellites in a direct ascent mode."[118] Although China's ASAT test did not exactly violate any existing arms control treaty, it broke a voluntary moratorium since the 1980s on such destruction of a satellite.[119] Further, the *Aviation Week & Space Technology* reported:

> US intelligence agencies calculated in advance that the Chinese were ready for the [intercept] and programmed American eavesdropping and space tracking sensors accordingly to obtain maximum information … US Air Force Defense Support Program missile warning satellites in geosynchronous orbit detected the Xichang launch of the ASAT kill vehicle, and US Air Force Space Command radars monitored the FY-1C orbit both before and after the intercept.[120]

However, China's anti-satellite test was not an anomaly, but an exemplar of a wide-ranging endeavour, to develop multiple war-fighting instruments in order to constrain America's ability to exploit space in an effort to produce a rapid and decisive terrestrial military victory over China.[121] It appears palpable that Beijing's investments in counter-space technology are driven by uncompromisable strategic concerns. In the near term, Beijing will focus on developing all possible means of defeating the superior conventional forces (read the US) it expects to encounter in any war over Taiwan.[122]

The PLA has been achieving critical knowhow regarding operational effectiveness as it gets capacitated towards exploiting space systems, in order to provide both information and capabilities that remain decisive vis-à-vis successful war-fighting. Given China's overall conventional weakness, counter-space operations are stressed upon in operational planning as an integrated element of its military response. The role of informationisation in future wars highlights the importance of space, electronic combat and computer network operations to fulfill the requisite demands of victory, including the potential scenarios of limited wars. China's investment in the realm of both space and counter-space efforts is likely to adversely affect Asian strategic equations and the military capabilities of the major players in the region in a far-reaching manner, as it would certainly expand the scope and magnitude of the battlespace.

Chinese objectives could be derived from a statement by Bao Shixiu, an analyst at the PLA's Academy of Military Science, when he argued that China does not have a clear space deterrence theory and that it seeks a limited capability to counter US dominance in space and reduce the likelihood of US attacks against space assets.[123] Nevertheless, Ashley Tellis affirms that although China is continuing to modernise and expand its military space capabilities, its efforts remain handicapped by significant deficiencies in technology; and China still remains constrained by the quality of its manpower base.[124] A US government report titled *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, released in October 2009, warns that China is ramping up its digital attacks on business and government computer networks. According to this Congressional Advisory Panel report, "China is likely to use its maturing computer network exploitation capability to support intelligence collection against the US government and industry,

by conducting a long-term, sophisticated, computer network exploitation campaign."[125]

Conclusion

It is evident that defence planning and implementation in the future has to incorporate the virtual world, in order to limit physical damage in the real one. As computer technology increasingly integrates itself into modern military organisations, including the PLA, military planners shall assign it the twin roles of being both a target and a weapon. Cyber forces are most likely to be integrated into an overall battle strategy as part of a combined arms campaign.[126] Modern military establishments, when involved in military hostilities, outline information superiority or information dominance in the battlespace as a key objective. The aim, in Clausewitzian terms, is to increase the 'fog of war' for the enemy and to reduce it for one's own forces—to be achieved through direct military strikes designed to degrade the enemy's information-processing and communications systems or by attacking the systems internally to achieve, not denial of service, but a denial of capability. In effect, this form of cyber warfare focuses almost exclusively on military cyber targets.[127]

Cyber warfare as a tool is well appreciated by the Chinese. In 2008, numerous computer systems around the world, including those owned by the US government, continued to be the target of intrusions that appear to have originated within the PRC. Although these intrusions focussed on exfiltrating information, the access and skill required for these intrusions are similar to those necessary to conduct computer network attacks. It remains unclear if these intrusions were conducted by, or with the endorsement of, the PLA or other elements of the PRC government. However, it is amply clear that developing capabilities for cyber warfare is consistent with PLA military writings on the subject. As India plans a $9 billion package for its IT roadmap, the Chinese threat indubitably looms large over the same.

As India gradually becomes more reliant on cyber space, added attention towards security of cyber space becomes even more palpably significant. National safety had to be ensured through securing the seas in the 19th century, through the air in the 20th century, and the coming 21st century

would demand securing the cyber space. As a consequence to recognising the security challenges of cyber space, the Indian government ought to stress upon the importance of a coherent approach, so as to insulate systems from being attacked by the adversary, by means of reducing risk and exploiting opportunities by improving comprehension and capabilities to secure its cyber space.

The Indian government could undertake the following measures: setting up a central cyber security command that would provide coherence to the entire programme; providing additional funding for developing innovative future technologies to protect Indian networks; developing and endorsing the growth of critical skills and integrating public sector, industry and civil liberties groups. Simultaneously, creating a security centre that could monitor cyber operations and undertake active monitoring of cyber space, coordinate incident responses and enable better understanding of attacks against networks. Thus, as China grows militarily and economically, its resultant strategies are all likely to expand, especially in the cyber warfare arena. Cyber war, in all probability, would assume the shape of being a key component and feature of any future conflict within Asia or beyond, as we step into the information age.

Notes

1. Qiao Liang and Wang Xiangsui, *Unrestricted Warfare: China's Master Plan to Destroy America* (Beijing: PLA Literature and Arts Publishing House, 1999), p. 144.
2. *Chao Xian Zhan: Dui Quanqiu Hua Shidai Zhanzheng yu Zhanfa de Xiangding* (Beijing: PLA Art Press, 2000).
3. For more details, see Ming Zhang, "War Without Rules," *Bulletin of Atomic Scientists*, Vol. 55, No. 6, November/December 1999.
4. Qiao and Wang, n. 1, pp. 144-45.
5. Ibid., pp. 10-11.
6. Ibid., pp. 122-23.
7. Xu Hezhen, "Focus on Psychological War Against the Background of Grand Strategy," *China Military Science*, (*Zhongguo Junshi Kexue*), No. 5, 2000, pp. 67-76, as cited in Foreign Broadcast Information Service-People's Republic of China (hereafter FBIS-CHI).
8. Avery Goldstein, *Rising to the Challenge: China's Grand Strategy and International Security* (Stanford, CA: Stanford University Press, 2005), p. 17.
9. Ibid., p. 12.
10. Sun Tzu, as discussed in Michael Pillsbury (ed.), *Chinese Views of Future Warfare* (New Delhi: Lancer Publishers, 1998).
11. Zhan Yu, "Strategic Considerations for Army Transformation," *China Military Science*, 25 August 2008, pp. 86-97, as translated and downloaded from the Open Source Center (hereafter OSC) website, document number CPP20080825563003.

12. Peng Hongqi, "A Brief Discussion of Using the Weak to Defeat the Strong under Informationized Conditions," *China Military Science*, No. 1, 2008, pp. 142-48, as translated and downloaded from the OSC website, document number CPP20080624563002.
13. For more details see, Li Deyi, "A Study of the Basic Characteristics of the Modes of Thinking in Informationized Warfare," *China Military Science*, 20 August 2007, pp. 101-05, as translated and downloaded from the OSC website, document number CPP20081028682007.
14. Richard D Fisher Jr., *China's Military Modernization: Building for Regional and Global Reach* (Westport, CT: Praeger Security International, 2008), p. 111.
15. Ibid., p. 112.
16. Wang Baocun and Li Fei, "Information Warfare," in Pillsbury, n. 10, p. 329.
17. Electronic warfare, as defined by the US Department of Defense, is any military action involving the direction or control of electromagnetic spectrum energy to deceive or attack the enemy. High power electromagnetic energy can be used as a tool to overload or disrupt the electrical circuitry of almost any equipment that uses transistors, microcircuits, or metal wiring.
18. For more details, see Clay Wilson, "Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues," Congressional Research Service (CRS) Report RL31787, 20 March 2007.
19. As cited in Wang and Li, n. 16.
20. People's Republic of China, *China's National Defense in 2008,* (Beijing: Information Office of the State Council, January 2009), p. 21.
21. Ibid., p. 22.
22. Qiao and Wang, n. 1, p. 9.
23. Views by Ming Zhou cited in "China Proves to be an Aggressive Foe in Cyberspace," *The Washington Post*, 14 November 2009.
24. As cited in John Arquilla and Solomon M Karmel, "Welcome to the Revolution…in Chinese Military Affairs," *Defense Analysis*, Vol. 13, No. 3, December 1997, p. 259.
25. James Mulvenon, "The PLA and Information Warfare," in James Mulvenon and Richard H Yang (eds.), *The People's Liberation Army in the Information Age* (Washington, D.C.: RAND, 1999), p. 180.
26. Ibid., pp. 183-85. Further, see Lu Linzhi, "Preemptive Strikes Crucial in Limited High-Tech Wars," *Jiefangjun Bao*, 14 February 1996, p. 6.
27. Wei Jincheng, "Information War: A New Form of People's War," cited in *Liberation Army Daily*, 25 June 1996.
28. NATO Parliamentary Assembly - Science and Technology Committee, "The Revolution in Military Affairs," November 1998.
29. Dai Qingmin, "On Integrating Network Warfare and Electronic Warfare," *China Military Science*, February 2002, FBIS-CHI, pp. 112-17.
30. Cited in Timothy L Thomas, *Cyber Silhouettes: Shadows Over Information Operations* (Fort Leavenworth, KS: Foreign Military Studies Office, 2005), p. 82.
31. Ibid., p. 84.
32. Ye Youcai and Zhou Wenrui, "Building a High-quality Militia Information Technology Element," *Guofang*, cited in FBIS-CHI, 15 September 2003.
33. As reported in *Mingpao News* and *Sun Daily News*, 05 November 2003.
34. Ibid.
35. Wang Jianghuai and Lin Dong, "Viewing Our Army's Quality Building from the Perspective of what Information Warfare Demands," *Jiefangjun Bao*, FBIS-CHI, 03 March 1998, p. 6.
36. Thomas, n. 30, p. 87.
37. For more on this subject, see Peng Guangqian and Yao Youzhi (eds.), *The Science of Military Strategy* (Beijing: Military Science Publishing House, 2005), p. 339.

38. Ibid., p. 340.
39. Dai Qingmin, "Innovating and Developing Views on Information Operations," *China Military Science*, cited in FBIS-CHI, August 2000, pp. 72-77.
40. For more details, see Office of the Secretary of Defense, *Military Power of the People's Republic of China*, Annual Report to Congress, 2004; also see, John Bennett, "Commission: US Should Push Beijing to up Pressure on North Korea," *Inside the Pentagon*, 17 June 2004.
41. Ka Po Ng, *Interpreting China's Military Power: Doctrine Makes Readiness* (Abingdon, Oxon: Frank Cass, 2005), pp. 110-11.
42. For more details, see Office of the Secretary of Defense, *Military Power of the People's Republic of China,* Annual Report to Congress, 2007.
43. Peng and Yao, n. 37, p. 345.
44. Ibid.
45. For more details, see "From Gettysburg to the Gulf and Beyond," by Colonel Richard J Dunn III, *McNair Paper* No. 13, 1992, quoted in *World Military Affairs Yearbook* (Washington, D.C.: Institute of National Strategic Studies, 1997), pp. 294-95.
46. Qiao and Wang, n. 1, p. 36.
47. Gurmeet Kanwal and Monika Chansoria, "Red Dragon Rising: China's White Paper Emphasises Offensive Defence," *CLAWS Issue Brief* No. 10, June 2009.
48. Thomas, n. 30, pp. 74-75.
49. Yang Liu and Wang Donghua, "Attention Should be Given to the Information Territory," *PLA Daily*, 03 December 2003.
50. Fisher, n. 14, p. 120.
51. James C Mulvenon, "Chinese Information Operations Strategies in a Taiwan Contingency," Testimony before the US-China Economic and Security Review Commission Hearing on *China's Military Modernization and the Cross-Strait Balance*, 15 September 2005.
52. Ibid.
53. Ibid.
54. Ibid.
55. Ibid.
56. Thomas, n. 30, p. 119.
57. Estimates by Andrew Yang and Glenn Schloss, "Mainland Cyber-Soldiers," *South China Morning Post*, 29 March 2001.
58. Timothy L Thomas, "China's Electronic Strategies," *Military Review*, May/June 2001.
59. As reported in the *PLA Daily*, 31 July 2003.
60. Peng and Yao, n. 37, p. 343.
61. Ibid.
62. Views expressed by Andrew Palowitch at the Georgetown University, "Cyber Warfare: Viable Component to the National Cyber Security Initiative?" 27 November 2007, http://cpass.georgetown.edu/43595.html, accessed on 30 November 2007
63. Cited in Stephen Fidler, "Steep Rise in Hacking Attacks from China," *The Financial Times*, 05 December 2007.
64. John Markoff, "China Link Suspected in Lab Hacking," *The New York Times*, 09 December 2007, p. A3.
65. Mark A Kellner, "China a 'Latent Threat, Potential Enemy': Expert," *Defense News Weekly*, 04 December 2006.
66. Cited in John J Tkacik, Jr., "Trojan Dragons: China's International Cyber Warriors," *Web Memo*, No. 1735, The Heritage Foundation, December 2007.
67. Ibid.
68. Richard P Lawless, Deputy Under Secretary of Defense for Asia-Pacific Affairs and Major

General Philip M. Breedlove, Vice Director for Strategic Plans and Policy, Joint Chiefs of Staff, Testimony before the House Armed Services Committee on "Recent Security Developments in China," 13 June 2007.

69. Ibid.
70. Cited in Mulvenon, n. 51.
71. As reported in the *Liberation Army Daily*, August 1999.
72. Julian E Barnes, "China's Computer Hacking Worries Pentagon," *Los Angeles Times*, 04 March 2008.
73. Gurmeet Kanwal, "Chinese Checkers," *The Financial Express*, 27 September 2009.
74. Wilson, n. 18, p. 10.
75. Indrani Bagchi, "China Mounts Cyber Attacks on Indian Sites," *The Times of India*, 05 May 2008.
76. "Is China Attacking Belgian Computers?" *United Press International*, 03 May 2008.
77. "India says Computers Hacked, but no Serious Loss," *Indo-Asian News Service*, 30 March 2009.
78. Kanwal, n. 73.
79. Thomas, n. 30, p. 84.
80. Bill Gertz, "China's Military Links Forces to Boost Power," *The Washington Times*, 16 March 2000, p. A1.
81. Regional Integrated Electronic System ('*Qu Dian*') - Project 995," *Sinodefense,* www.sinodefence.com/electronics/c3i/qudian.asp, accessed on 28 January 2007.
82. Peng and Yao, n. 37.
83. Li Daguang, *Space Warfare (Taikong zhan)* (Beijing: Military Science Press, 2001).
84. Hou Yan, Cheng Qinghua, and Geng Yandong, "Space Power Support of Integrated Joint Operations," (*Kongjian liliang zhichi xia de yitihua lianhe zuozhan*), *Journal of the Academy of Equipment Command and Technology* (*Zhuangbei zhihui jishu xueyuan xuebao),* October 2005, p. 48.
85. Views by Larry M Wortzel, "China Space Briefing," cited in Ashley J Tellis, "China's Military Space Strategy," *Survival*, Vol. 49, No. 3, Autumn 2007.
86. Ashley J Tellis, "China's Space Capabilities and US Security Interests," *Quaderni di Relazioni Internazionali*, October 2008.
87. Views expressed by Kevin Pollpeter in Tania Branigan, "China Launches Manned Spacecraft," *The Guardian*, 26 September 2008.
88. Tellis, n. 85.
89. For more details, see Gil Siegert, "The Chinese Space Program," Unclassified Working Paper, Commission to Assess the Ballistic Missile Threat to the United States, Federation of American Scientists, July 1998.
90. For more on this issue, see "China's Space Capabilities and their Impact on US National Security," Testimony by Ashley J Tellis, before the US-China Economic and Security Review Commission, "China's Proliferation Practices, and the Development of its Cyber and Space Warfare Capabilities," Washington, D.C., 20 May 2008.
91. Mark A Stokes, *China's Strategic Modernization: Implications for the United States* (Carlisle, PA: US Army War College - Strategic Studies Institute, 1999).
92. Tellis, n. 90.
93. Office of the Secretary of Defense, *Military Power of the People's Republic of China*, Annual Report to Congress, 2009, p. 52.
94. Bao Shixiu, "Deterrence Revisited: Outer Space," *China Security*, Vol. 3, No. 1, Winter 2007, p. 9.
95. Chinese scholar Dingli Shen admits that China's anti-satellite test was undertaken "purely for the purpose of breaking the US space hegemony." For more details, see Dingli Shen, "The Logic of Hegemony," published as 'Shen Dingli Rebukes Pentagon Report on PRC

Military Power, Questions Its Logic,' OSC CPP20070530050001, *Jiefang Ribao*, 29 May 2007.

96. Transcript of the Testimony of General James E Cartwright, Commander, US Strategic Command, before the Strategic Forces Subcommittee of the Senate Armed Services Committee, Russell Senate Office Building, Washington D.C., 28 March 2007.
97. Mary Fitzgerald, "China's Predictable Space 'Surprise'," *Defense News*, 12 February 2007; also see, Mary Fitzgerald, "China's Military Modernization and its Impact on the United States and the Asia-Pacific," Statement on China's Military Strategy for Space before the US–China Economic and Security Review Commission, 30 March 2007.
98. Ibid.
99. Cited in Edith M Lederer, "Chinese Colonel Sees Arms in Space," *The Washington Times*, 27 January 2007.
100. Tellis, n. 85, p. 52.
101. For more on this subject, see Brian Harvey, *The Chinese Space Programme: From Conception to Future Capabilities,* (New York: Wiley, 1998); Joan Johnson-Freese, *The Chinese Space Program: A Mystery Within a Maze,* (Melbourne, FL: Krieger; Publishing, 1998); and Kathryn L Gauthier, "China as Peer Competitor? Trends in Nuclear Weapons, Space, and Information Warfare," *Maxwell Paper* No. 18, (Maxwell Air Force Base, AL: Air War College, 1999).
102. Stokes, n. 91, p. 118.
103. Office of the Secretary of Defense, *Military Power of the People's Republic of China*, Annual Report to Congress, 2002, p. 32.
104. Office of the Secretary of Defense, n. 93, p. 52.
105. Hong Bing, et al., "The Weaponisation of Space – A Call to the Danger," (*Taikong Wuqihua – Yige Weixian de Xinhao*), *Jiefangjun Bao*, cited in the *PLA Daily*, 12 December 2001.
106. Cited in *Jiefangjun Bao*, *www.pladaily.com*, 04 November 2002, accessed on 06 June 2009.
107. Tellis, n. 85, p. 64.
108. Tellis, n. 86.
109. Ibid.
110. Tellis, n. 90.
111. Tellis, n. 86.
112. "Ensuring America's Space Security: Report of the FAS Panel on Weapons in Space," (Washington D.C.: Federation of American Scientists, 2004), pp. 17–18.
113. For a useful overview, see "2005 Space Almanac," *Air Force Magazine*, Vol. 88, No. 8, August 2005, pp. 44–64.
114. For more details, see "Beam Energy Weaponry as Powerful as Thunder and Lightning," *Jiefangjun Bao*, cited in FBIS-CHI-96-039, 25 December 1995.
115. "PLA said Developing Anti-Satellite Weapons to Counter US NMD, TMD Systems," *Hong Kong Ming Bao,* 30 January 2001.
116. Tellis, n. 86.
117. Craig Covault, "China's Asat Test Will Intensify US-Chinese Faceoff in Space," *Aviation Week & Space Technology*, 21 January 2007.
118. Geoffrey Forden, "A Preliminary Analysis of the Chinese ASAT Test," *Massachusetts Institute of Technology*, http://web.mit.edu/stgs/pdfs/A%20Preliminary%20Analysis%20of%20the%20Chinese%20ASAT%20Test%20handout.pdf, p. 29, accessed on 22 January 2007.
119. It should be noted that the Outer Space Treaty (OST) of 1967 bans the deployment of weapons of mass destruction in orbit, on the moon, or otherwise in outer space; and limits the use of the moon to peaceful purposes.
120. Ibid.
121. Tellis, n. 85, p. 60.

122. For more details, see Richard C Bush and Michael E O'Hanlon, *A War Like No Other: The Truth About China's Challenge to America,* (Hoboken, NJ: John Wiley & Sons, 2007).
123. Bao Shixiu, "Dominance in Space," *Beijing Review*, 15-21 March 2007.
124. Tellis, n. 86.
125. Cited in Rupert Taylor, "Chinese Cyberspace Sabotage: Beijing Accused of Digital Attacks on Sensitive Networks," *Global Security* (Online Edition), 12 November 2009.
126. For more on this subject, see Timothy Shimeall, Phil Williams and Casey Dunlevy, "Countering Cyber War," *NATO Review*, Winter 2001/2002.
127. Ibid.