Behind the Great Firewall of China: A Look at RMA/IW Theory From 1996-1998

by Mr. Timothy L. Thomas
Foreign Military Studies Office, Fort Leavenworth, KS.

November 1998

Military specialists in China have monitored the progress and studied the societal and military impacts of the current revolution in military affairs (RMA) for some time. For example, they studied closely Russian Marshall Nikolai Ogarkov's works and observations on the RMA during the 1980s. Chinese specialists also studied not only the application of new technologies by the multinational coalition during Desert Storm in 1991, but also their impact on military art.

These studies greatly influenced the initial examination, assessment, and development of China's RMA approach, as well as sub-components such as information warfare (IW). The struggle now is to develop a uniquely Chinese approach, one that integrates Chinese military philosophy and history, developments in modern technology, and the study of foreign army experiences. An example of a uniquely Chinese approach can be found in the 1985 monograph of Shen Weiguang, then a 25-year-old soldier of the Chinese ground forces. In one of the first papers ever written on IW, Weiguang described the concept of **"take-home" battle** in which the Chinese would conduct a different and personal type of People's War with computers:

> those who take part in information war are not all soldiers. Anybody who understands computers may become a "fighter" on the network. Think tanks composed of non-governmental experts may take part in decision-making; rapid mobilization will not just be directed to young people; information-related industries and domains will be the first to be mobilized and enter the war...[1]

At every opportunity authors and leaders are stressing the requirement to develop asymmetrical or "out of the box" thinking, such as this excerpt from analyst Li Yinnian:

> we should go for the enemy's weak parts and dead angles. Technologically, we should try harder to go where others have not trodden and develop uncommon technology. We can also consider organizing some **"network special warfare detachments"** and finding some computer experts to form a shock brigade of **"network warriors"** who specialize in looking for critical nodes and control centers on the enemy network and sabotaging them.[2]

By striking at the vital points of an enemy's information and support system, attacking forces become blinded and paralyzed and their morale collapses.[3]

This article examines the Chinese understanding of the RMA, its information warfare corollary, and the impact of these issues on the Chinese understanding of future war. The focus is on the years 1996-1998, with the research designed to identify significant changes. It centers on those areas that are unique to the Chinese understanding of the RMA and IW, and areas of concern to the West.

Defining the RMA

Chinese military analysts recognize that a military-technological revolution (MTR) has occurred, citing the whole host of new technologies used during operation Desert Storm. In the opinion of most Chinese specialists, a far-broader RMA, encompassing the MTR, is still in progress and far from complete (some analysts, for example, believe the RMA will be complete only by 2050 while others see a completion date somewhere between 2005 and 2010).[4] This RMA, they point out, is the natural result and progression of social, economic, and science and technology developments associated with the information age. It is not known if the economy of China and other countries can support this revolution completely. It is also unknown what effect other technologies and sciences, such as biology, will have on the present RMA. Thus, while the revolution eventually will lead to significant changes for the armed forces of China, they must be content in the short term, as many other armies must be, with the current weapons and equipment of the Chinese armed forces supplemented with a few new weapons; and new combat and training tactics that supplement the current technology gap, much as Sun-Tzu and Chairman Mao accomplished during the agricultural and industrial ages, respectively. These developments will be followed later by changes in equipment, troop strength, strategy, tactics and training.

Further, the Chinese characterize the present RMA as fundamental, all-inclusive, extensive, unbalanced, and protracted. It is fundamental in that it represents a transformation of the military establishment from an industrial to an information era. It is all-inclusive in that it touches on every sphere and aspect of military development. It is extensive in that it is taking place all over the world but unbalanced in that it is not taking place simultaneously with the same intensity everywhere. And it is protracted in that it has a start point but no clear-cut end point. In the opinion of some Chinese analysts, this revolution, which started in the civilian sector, will extend to the military sector after building sufficient "potential energy."[5]

The Chinese have been reluctant to offer their official definition of the RMA, relying instead on Western definitions of the term. One definition of the RMA not available in the press but reportedly from the 1997 Chinese military affairs dictionary defined the **RMA** in the following way:

> starting from the premise that social transformation is a prerequisite for a revolution in military affairs, the military field experienced a series of fundamental and profoundly influential transformations. It is primarily a reflection of qualitative changes in military technology, weapons and equipment, unit structure, warfighting methods, and military thought and theory.[6]

The Chinese Military Affairs Dictionary, 1990 version, does not have a definition of RMA but defines **military affairs** as

> Involving both theory and practical matters related to armed combat. For example, it includes the construction of armed forces, the preparation for armed conflict, and the research into military science. It also includes both social, political, and economic aspects. During the long period of war, people deepen and broaden their knowledge of military affairs, making military affairs the embodiment of a science with wide-ranging meaning.[(7)]

The Chinese apparently utilize the term "military revolution" interchangeably with and more often than RMA. A 1996 Chinese article on IW theory, for example, defined a **military revolution** as "a reflection of social, economic, and scientific and technological changes in the military field."[(8)] Information technology (IT), the article added, has given rise to this new, worldwide military revolution. IT is the "core and foundation of this military revolution, because information and knowledge have changed the previous practice of measuring military strength by simply counting the number of armored divisions, air force wings, and aircraft carrier battle groups. Nowadays, one must also take into account some **invisible forces**[(9)], such as computing capabilities, communications capacity, and system reliability."[(10)] Another 1996 article defined a **military revolution** as "a major qualitative change which can correctly integrate, in good timing, advanced technologies and weapon systems with new military theories and military establishments; bring permanent changes to modes of operations; considerably improve military efficiency; and enhance the combat effectiveness of armies by several orders of magnitude."[(11)] To improve efficiency and effectiveness, the challenge of the military revolution is finding a way to combine the increased accuracy of technology with the increased complexity required by new military theory/strategy. Simple force ratios built on numbers of pieces of hardware have lost their significance. Accuracy, however, has many problems to overcome, especially since there is five to ten times the amount of information to handle, and the information has a quality all its own. The good information must be separated from "information contamination or information trash." Theory must be directed at the art of dealing with information at higher levels where accuracy is hard to achieve, at the level of multidimensional battlefields and commanding diversified forces via multi-media devices (computers, images, etc.).[(12)]

A third definition of a **military revolution** developed in 1996 noted that it consists of three factors that must be integrated: advanced weapons systems, pioneering military theory, and corresponding force organization. These changes are designed to raise a country's military capability to its maximum potential. In-depth precision strikes will be the key combat form, requiring the creation of a joint operations theory, while concepts such as a nonlinear battlefield and **non-contact combat** will dominate. Offensive-defensive IW will be the focus of coming wars. The aim of belligerents will be to seize the information high ground and pave the way for ultimate victory, with the struggle for information supremacy becoming the crux of battle, in a sense acting as a strategic deterrent.[(13)]

Two years later, the tone and substance of Chinese articles on the RMA had changed. One article noted that "a mammoth revolution currently underway in the military sphere is producing an unprecedented impact on, and shock waves in, man's military activities."[(14)] Another noted that a "new military revolution is now taking the world by storm."[(15)] The military revolution this author speaks about sounds very familiar to the RMA:

> the history of the development of mankind shows that the development of science and technology from a quantitative change to a qualitative change and the achievement of a "qualitative leap" invariably led to a revolutionary change in the form of the technology era of mankind and triggered off a profound military revolution.[(16)]

Engels, the author noted, pointed out over 100 years ago that technology determines tactics. Qualitative changes in technology and weapons cause changes in military theory and the composition of the force. The initiator of the military revolution currently underway among these three (weapons systems, theory and organization) was the military-technical aspect of the weapon systems in their physical form.[(17)] Later, military **theory becomes the soul of the military revolution**. In some information societies, military theories have already overtaken military technologies as the leading factor. The military revolution is completed when all-round changes are reflected in organization, structure and the setup of the military system. Military revolutions thus follow the trend of moving **"from objects to concepts and from concepts to structure...its ultimate completion will change the mode of military activities in the complete sense and bring about a qualitative leap in combat capability...and we can put a full stop to the new military revolution."**[(18)]

A military revolution can effect policymakers, both military and non-military alike. Precise kills allow policymakers to flexibly use both diplomatic and military means to political and strategic ends. Information as a diplomatic or combat resource permits global reach, nonlinear warfare, speed of light transmissions, comprehensive integration, and multiple and joint use. Diverse technologies indicate that single weapons alone will not be the key factor in judging combat capability but rather the comprehensive performance of basic weapons "systems." Finally, new theory and force organization (to include the impact of the RMA on training) must be developed.

China's most prolific writers on the RMA note that the country must find its own "unique techniques and skills" during its investigation of the RMA. The country should not simply follow western thinking and add only western developments and technologies to the existing framework since

> due to their different economic and scientific development levels, as well as their different cultures, traditions, and ways of thinking, different countries will be subjected to different impacts produced by military revolutions; as a result, they will adopt different approaches toward new things and accept the new military revolution in varying degrees. Therefore, there will be a **growing trend toward diversification in the pattern of war at the initial stage of the military revolution**.[(19)]

Impact of the RMA on Chinese Theory and its Organization/Training for Warfare

The RMA has had a significant impact on the way in which Chinese military authors view and assess military theory and today's battlefield. The Chinese note that the objectives are more limited, in that total surrender or occupation of enemy territory are not as important as in the past. The struggle to control information is more sharp and fierce than ever before, the battlefield is more transparent due to the digital technology that extends the range at which forces can be detected, warfare is highly integrated (especially between land, sea, air, and space forces), and the lines of demarcation between strategic, campaign and tactical operations are more blurred with each passing day.[(20)]

The understanding of the word "warfare" has changed as well, in that the information age has introduced more potential instigators of warfare than ever before (to include terrorist organizations, drug cartels, etc.). The face of war has changed from mechanized to information and precision warfare, and the duration of war is being shortened. The time to make decisions and implement them has also shrunk, and there is an effort to avoid life-and-death decisive battles if casualties can be spared by other methods. Finally, the meaning of "concentration of forces" is moving from the tactical to the campaign and strategic level of war.[(21)]

The Chinese military, these authors contend, is intent on exploiting the advantages offered by the information age and its new technology. Information technology (IT) has provided five capabilities on the modern battlefield: stereoscopic displays; wide-ranging reconnaissance and surveillance; very deep, high-density early-warning networks; accurate positioning systems that cover the entire globe; a wide variety of information communication methods with anti-interference capabilities; and nimble, high performance automated battlefield controls. These systems have become the nervous system of the warfighting effort and exert a multiplier effect on warfighting capabilities. Combat strength is a combination of personnel, weaponry, information, and the integration of these elements. They also recognize that the **ability to control information resources, both friendly and enemy, will determine victory or defeat, as well as the ability of information capabilities to break the enemy's will to resist (by attacking his cognitive understanding and convictions)**.[(22)] IT has blurred the once sharp dividing line that separated peacetime and wartime actions.

IT has also caused significant changes in weaponry. In the past, matter and energy were the two main components, whose primary capabilities were mobility and lethality. With IT as their anchor, new high-tech weapons pursue the integration of matter, energy, and information, which allows weapons to be "smart" and "configurable." IT based weapons are also more effective, a trait demonstrated during Desert Storm where, by Chinese calculations, precision-guided munitions accounted for only 7% of the munitions launched but destroyed 80% of the total targets. Finally, IT has shown that force calculations are now less devoted to quantity and more devoted to quality.[(23)] Stated somewhat differently, **invisible forces** (computing capabilities, communication capacity and system reliability) are now as important in **measuring military strength** as the number of divisions, wings and battle groups.[(24)]

Organizationally, the RMA should result in a scaled down force in both personnel and numbers. Quality will replace numerical strength. Equipment will become more compact and integrated, designed to operate in one unified, organic operational space. "Tree-shaped" command systems will be replaced by "network-shaped" command organizational systems. Priority will be given to reconnaissance equipment, information weapons systems, and the development of a battlefield information network based on computer technology. Training methods must also change, and the introduction of simulation laboratories designed to strengthen research, forecasting, and the integration of technology and tactics are priority items. Finally, people must be educated in the field of IW. The goal of this entire effort is to "unify the concept of a people's war with the concept of victory through information."[25]

One of the most important corollaries to evolve out of this military revolution is that associated with information war. IW was defined in a 1995 article by two senior PLA Colonels as:

> combat operations in a high-tech battlefield environment in which both sides use information-technology means, equipment, or systems in a rivalry over the power to obtain, control and use information. Information warfare is combat aimed at seizing the battlefield initiative; with digitized units as its essential combat force; the seizure, control, and use of information as its main substance; and all sorts of information weaponry [smart weapons] and systems as its major means. Information warfare is combat in the area of fire assault and operational command for information acquisition and anti-acquisition; for suppression [neutralization] and anti-neutralization; for deception and anti-deception; and for the destruction and anti-destruction of information and information sources.[26]

IW will affect Chinese views of combat since the fight for information dominance is so intense. Additionally, outer space, force engagement times, and the types of force concentrations (from people to firepower at the campaign and strategic level) must receive attention.

The remainder of this essay studies the content of China's IW thinking. It examines the thoughts of the Chinese author who claims to have first written about information warfare, and follows with an examination of Chinese writings on the subject of IW from 1996-1998.

A Look at the Information Warfare Thoughts of Shen Weiguang

In 1995, Dr. Shen Weiguang, author of more than 100 articles (and mentioned above as one of the first authors to write about the topic of IW), wrote an IW introductory research piece for the Chinese military newspaper JIEFANGJUN BAO. His thoughts offer a touchstone from which to measure more recent IW writings in China.

Weiguang defined information warfare as command and control warfare or **decision control warfare**, using information as the main weapon to attack the enemy's cognitive and information systems, and to influence, check or change the decisions of enemy policymakers and their consequent hostile actions. That is, the main target of IW is the ability to disrupt the enemy's cognitive and trust systems, and to exert control over his actions. This definition implies that U.S. and Russian concepts of perception management and reflexive control, respectively, are also of interest to the Chinese, since control is a primary function of each. The Chinese sometimes refer to this idea as "guidance control." Here the term cognitive system refers mainly to information and computer decision-making systems. This thinking is similar, Weiguang notes, to a U.S. air force colonel who recommended "electronic beheading" at the beginning of an IW operation.[27]

IW has changed not only the pattern and methods of war but also its form, according to Weiguang. For one thing, IW will be carried out though the army and society as a whole, a new application of a People's War. Non-governmental organizations in society and individuals will make use of the global computer network to take part in IW. This will make it increasingly difficult to define where and who are the belligerent parties on the information battlefield since the latter now has nearly unlimited parameters. Computer programmers will return to their offices or homes to fight, denying servicemen the chance to engage in close combat. "Unity of a nation" is the source of power in such a war, where the people are extensively mobilized. Soldiers must also become more well-rounded in this environment, with expertise not only in military affairs but also in science and technology. Human policy decisions rather than technology remains the key to victory.[28]

IW also will give rise to a revolution in military philosophy, such as the fact that information superiority has replaced air superiority in four-dimensional warfare, offering a new criteria for freedom of action. IW will attempt to gain the initiative in battle through control over information flows, especially regarding intelligence. The operational target of IW lies precisely in control rather than bloodshed. The Chinese, Weiguang notes, have proposed maneuver warfare and **structural damage warfare** in their tactical studies. The former is distinguished from mobile warfare since it "takes IW as its soul." Structural damage warfare can only become effective when information warfare's true essence is understood, that is when it is brought in line with IW's entire framework. Weiguang also proposed that multi-layer and pagoda-style command systems be abandoned, with an increase in the intermediate command layers leading to a more balanced command system.

Weiguang warns not to abandon all thinking from the past. He notes that in accordance with the theory of the "negation of the negation" of historical development, IW will negate much of the theories associated with mechanized warfare of the industrial age. But IW will seek reference from the theory of military tactics, which predictably lies in the military science of Sun Tzu. He adds that IW, combined with Chinese thinking on guerrilla warfare, will display tremendous power. Additionally, **small information units** will carry small-size, light comprehensive electronic equipment offering navigation and night vision capabilities, as well as the capability to release information bombs. These units will be composed of small groups of soldiers active in the enemy rear, implying not only a continued but **expanded role for special forces soldiers** in the IW environment. The **losers** in future wars will be those who lack command thinking and the ability to apply strategies, not those who possess only backward technology. System inputs from grasping or attaining knowledge costs far less than directly purchasing advanced weaponry.[29]

The correct choice here is avoiding the opponent's strong points and attacking its weak points, making the best use of advantage and avoiding disadvantage. When faced with a technologically superior force armed with IW weaponry, it is important to refrain from "devising a solution only from the angle of tactics and stratagem." Instead, the thinking of technological experts can help turn one's strategic thinking or theory to advantage, finding new technological orientations for strategy and tactics. As such, emphasis must be placed on **military soft science**, which utilizes soft attacks and soft damage. Military soft science is

> A branch of science devoted to the study of military theory, strategy, planning and management. The study of soft science is a comprehensive one that straddles the army, various departments, and branches of science. IW involves not only computer virus warfare and EW, but also psychological warfare, deterrence warfare, and political propaganda warfare....[IW] is beyond comparison to all previous forms of warfare. Therefore, it calls for the support of "hard" science as well as the guarantee of "soft" science.[30]

Weiguang recommends that China not sit and wait but start with military soft science and move out on its own path of development, stressing the need for cross fertilization and cooperation of qualified people from multiple branches of science.

Views on Information War (1996)

In 1996 there was a focus on the high-technology aspect of IW, especially the digitalization aspect. There were also thoughts expressed on information injuries, negative entropy, U.S. and other foreign army IW efforts, IW's impact on military art, and People's War. Finally, there was much conjecture on how technology could be transformed into theory.[31]

The Chinese army in 1996 believed that IW was the focal point of the new military revolution. It is clear that IW will have a much larger operational space in which to maneuver than EW had. The Chinese believe that the precondition for the conduct of IW is to be found in the digitization of the battlefield and the armed forces. Digitalization, in the view of one author, would

> turn voices, characters, images, and information of various types into digital coding; link together battlefield command posts, various operational and logistic detachments, single-piece weapons and equipment, and individuals through such transmission means as wireless stations, optical-fiber telecommunications, and satellite telecommunications; form an intertwining computer telecommunications network; ...realize near-time information exchange in all directions; ...and will optimize the command and control functions of our units so as to enhance their antipersonnel force, survival capability, and ability of co-ordinated operations. Therefore, **battlefield digitization will be a background condition and a core pillar for conducting and winning the information war**.[32]

Digitized forces can enhance the fighting capacity of a force simply by changing the way information is transmitted. To counter this problem, the following techniques should be used: insert information into a network; interfere with viruses; destroy vital nodes; and employ dispersed forces and strength, breaking up the enemy into horizontal and vertical parts.[33]

Information was viewed in 1996 as a weapon that could cause various types of injury. These "information injuries" were caused by deception, occupation (information overload), contamination, blocking or sabotaging, and guidance.[34] The latter is so named because it intentionally transmits certain information to an opponent so as to cause him to take an action conforming to the opposite side. Guidance injury is thus much like the U.S. perception management theory or the Russian reflexive control theory mentioned above. The target of these different types of "information injuries" is the enemy's cognitive system and information system. Here the author defines a cognitive system as referring to a man's brain, thinking and information analysis process which can be affected by deception, contamination and guidance injuries. An information system refers to the collection, handling and transmission of information by communications systems, news media, and computer hardware and software, which is susceptible to deception, occupation and contamination.[(35)] Direct information attacks affect the decision-making and command authorities of an enemy, while an indirect attack affects enemy morale and incites anti-war sentiment, eventually rendering the enemy command ineffective.

Another author noted that the essence of information is the negation of uncertainties, or **negative entropy**. Entropy is disorder, thus negative entropy means order. This means that areas with the greatest uncertainties will have the greatest demands for information. Whoever can turn uncertainties into certainties will gain the upper hand under such conditions.[(36)]

One of the more interesting articles of 1996 discussed military art. Author Ch'en Huan first discussed the challenge to traditional operational principles, noting that force concentration is no longer effective, replaced by the concentration of striking efficacy in the form of information and other types of energy; that the role of software is increasing; and that a soft strike force is now even more important than a hard strike force. Additionally, he noted that the lines between front and rear will blur, with attacks perhaps aimed at the support and technical units first and then the first echelons, and with the operational objective being to paralyze the other sides information system and will to resist. Long range combat will replace hand to hand fighting, and new space weapons will appear in a "continuous stream": laser, ultra-high frequency and ultrasonic wave weapons; mirror-beam, electromagnetic and stealth weapons; plasma, ecological, smart, logic, and sonic weapons; and electromagnetic guns. Finally, Huan noted that command structures would be "thin and flat" since networked systems would eliminate the need for middle-level commanders, reducing the number of levels and producing a structure that is wide horizontally and short vertically.[(37)]

The idea of a People's War also found expression in 1996. One author noted that there would now be a new kind of political mobilization, one based on "generating and distributing political mobilization software via the Internet, sending patriotic e-mail messages, and setting up databases for traditional education." These factors greatly increase the ability of people to participate in future wars, aiming to maintain the "peace of hardware through software confrontations."[(38)]

Chinese authorities also wrote often on the IW developments and practices of the United States. Even though countless detailed accounts had already been written about the U.S. based coalition victory during Desert Storm, and how IT played such a key role in the success of that operation, more articles continued to appear. The overwhelming majority of comments about the U.S. approach to the RMA and its IW corollary were positive. The Chinese commentary was rather matter of fact, simply stating a success as a success and not entering into polemics about what the U.S. might do with its success. However there exists some material on how "foreign armies" might conduct an IW attack. For example, one report noted the following warfare plans:

- virtual reality warfare (applying virtual scenes of troops advancing or withdrawing, or transplanting virtual information into an enemy's command and control system for a variety of reasons, such as disinformation, deception, disruption, or to cause panic)
- computer virus warfare (to paralyze core equipment)
- network warfare (designed to infiltrate information systems)
- broken circuit warfare (designed to disrupt the flow of command and control information)
- information infiltration warfare (designed to sap enemy morale by sending information directly to soldiers about the military and civilian situation, sending information from soldiers at the front or rear to civilians, and so on reaching not only commands but the individual soldier very quickly and silently while offering a more extensive and destructive force than the old methods of PSYOP).[39]

There have been some Chinese warnings to the U.S., although they make up only a small percentage of the reporting on the issue (especially compared to Russian military journalists, who speak with emotion, almost hysteria, and who have accused the West of preparing for IW with Russia on several occasions). Chinese criticism is worth U.S. attention in any case, since it is usually professional in manner, and the specialists can decide for themselves if the Chinese have made good recommendations or not. For example, one author noted that the U.S. Army must be careful since it can easily become trapped in the blind alley of technology. Whereas transparency can be enhanced by advanced technologies, there is no way of making the decisions of commanders as transparent as the view of the battlefield, the author notes.

By the end of 1996 the following questions were being asked: Will the guiding RMA ideology be pulled by theory or practice? How will practice be reflected in the reworking of the strategic plan? How can war methodologies be reformed and updated? One author noted the need to improve "the theories and methods of war, so as to bring along and guide the practice of army building." In this regard, simulation confrontation technologies were an extremely urgent area in need of development. Combat laboratories, one author believed, must be built to take advantage of virtual reality technology which allows military science to come closer to the natural sciences in its ability to discover, test, and verify the rules of military science. The same author noted the further need for a macro-control system. This is because not only the armed forces, but various departments of the entire country could experience profound changes. The development of an overall system would allow for targets, content, methods, and measures of the RMA to be guided in its implementation. At the same time, the enhanced role of the individual was underscored, especially at the soldier level where a wide range of professional skills are employed.[40]

Views on Information War (1997)

In 1997, the theory of IW was developed, and a IW exercise was held late in the year. It was one of the first applications of theory to field conditions. Increased emphasis was placed on finding ways to use operational thinking in the most effective way. The idea of "confrontation of commands" played a key role in the discussions of the face of future war, and the concept of information security was also developed. Finally, a plan was offered to build an information-age China.

In one 1997 article, IW was defined as

> all types of war fighting activities that involve the exploitation, alteration and paralysis of the enemy's information and information systems, as well as all those types of activities which involve protecting one's own information and information systems from exploitation, alteration and paralysis by the enemy.[41]

This definition appears to closely resemble U.S. definitions at the time. Author Liang Zhenxing then went on to explain that the essence of IW theory, from his point of view, is to render operational space cloudy and indistinct to the enemy while making operational space transparent to one's own force. IW was described by Zhenxing as a style and not a category of war, and something that cannot function as a stand-alone item. He characterized mobile warfare, land warfare, guerrilla warfare, and electronic warfare as styles of warfare.

The IW highlight of 1997 was a late autumn IW exercise in the Shenyang Military Region. This exercise involved the deployment of ground, logistics, medical, and air force units. As one observer noted:

> the speed of marking and mapping on the computer screens by the advisors was more than 20 times faster than the traditional manual methods, and accuracy was 100 percent [faster]. The computer network in the commanding unit was activating more than 100 terminals, connecting and commanding a fourth-degree campaign network...the commanders' attention was not on the number of documents handled, but on whether the high-tech design was excellent. Their focus was not on whether the commanding procedures and soldiers' movements were standardized, but on how much high technology was being applied to their strategies and operations.[42]

The Taiwan Central News Agency on 27 December published a report on the exercise, and accused the People's Liberation Army (PLA) of trying to develop a computer-virus warfare capability.[43]

A few weeks later in the "Military Forum" column of JIEFANGJUN BAO, the PLA Academy wrote a detailed article on the confrontation of command on the information battlefield.[44] The **initiative in future battle**, the work concluded, depended on the side that controlled information. The seminar then went on to discuss the contours of an information engagement, noting that it would probably start with a confrontation of command. PLA Academy Commandant Guo Anhua noted that the **success of a military revolution depends not on technology but rather on operational thinking and the methodology of utilizing technology in the most effective way**. No longer is it enough to shape an opponent's decisions through stratagem, firepower, and the indirect approach, since now the direct approach is possible. Confrontation can only be understood from the integration of technologies, and from "winning in strategy by winning in battle" simultaneously (instead of the old "winning in strategy via strategy" or "winning in strategy after winning in battle"). Troop deployments are oriented more on the communications between an enemy's command system and his combat units than against manpower and firepower, as the former destroys the ability to deploy troops. Finally, confrontation of commands manifests itself as a confrontation on the information network, which allows for joint and integrated operations.(45)

To obtain network supremacy, one must have superiority in the procurement, transmission, and processing of information. That is, network supremacy is possible only if it exists at these three levels. The "**drift mobility**" of command, the fact that the number of control nodes for command has redundancy built-in, makes it harder to cut off the head (a U.S. division commander in the 1980s was able to communicate from any of 14 network nodes across the division). Networks able of performing on the battlefield are time intensive and must be planned well in advance since they take years to construct.(46)

Another characteristic of the confrontation of commands (or information engagement) is the fact that human intelligence stands between two technologically based "bodies of knowledge", that is two computer-based systems. The human must be able to comprehend what happens when these two bodies of knowledge collide, and how to control or manipulate the interaction and the consequences.(47) Humans must respect technology but not deify it, neither blindly following the RMA and IW theories nor evading its challenges.

Yet another characteristic is the fact that computer-aided simulations are used more and more in decision-making for the confrontation of commands. Network models calculate combat time, the distribution of manpower and weaponry, a comparison of battle plans, and an evaluation of combat effectiveness, with the totality designed to arrive at a scientific prediction and a decision. But the human interface maintains its importance here too since "how to think" and analyze may be more critical than how to do something suggested by a computer. The Chinese regard their efforts in this area as lagging behind foreign armies, noting that a lack of experimentation has not allowed them to "know the flavor of the pear."(48)

Finally, and perhaps most important, the confrontation of commands must no longer be viewed as simply a confrontation between two systems designed to support operations. Rather, the **command functions** have become so crucial to survivability that they **must be outfitted with their own innate attack and defend systems**. Command structures must also be careful not to follow in someone else's inertia, or to follow the inertia of tradition too closely. A unique approach to the subject is vital to success. Additionally, the material base of the command confrontation, technology, must achieve breakthroughs in some of the critical technologies for future success.(49)

A detailed article on computer virus weapons also appeared in 1997. A computer virus was defined by the author as a computer program which can revise a computer's program or use a replica of itself to infect computer systems other than the one already invaded. A virus revises or destroys a computer system after normal applications have been executed. Not only can a virus alter stored data, revise stored files, and cause computers to have "mental disorders," according to the Chinese, but it can paralyze an entire computer network without anyone knowing about it. More than 6,000 executable, infectious, destructive, hidden, latent or aggressive viruses were listed.[50] The author further noted that **computer viruses** may become a **new field for electronic countermeasures**. Viruses can attack the brains of an operational command system, not just the receivers and transmitters, as occurs with normal electronic countermeasures. In the latter case, electronic measures can continue once jamming ceases. This is not the case with a virus. It can cause permanent damage. Insertion remains a problem, of course, but with the assistance of electromagnetic waves, they can be inserted remotely into airplanes, tanks, submarines and other systems.[51]

Chinese methods of countering viruses to date include:

- establishing a native integrated circuit production industry
- establishing secure importation procedures for computers brought into the country
- studying computer virus detection methods, establishing mechanisms for defending against viruses and improving the ability of computer systems to resist viruses
- reinforcing and strengthening the resistance of systems to electromagnetic pulses
- tightening computer systems' use and management, and the awareness of the potential of information confrontation.[52]

These recommendations will help guarantee the national security strategy of China, its overall military information system security, and raise the consciousness of the citizenry in regard to the information security of the country. China must, as a result, draw up security standards and norms for its information infrastructures; enhance research on information protection technology, and develop technologies to detect, track and prevent computer network incursions; and independently develop computer systems to raise the technological level of China's independent efforts in this area. High-level bodies designed to establish national defense information modernization are required. They must track trends in foreign IT and IW, develop a strategy for China's defense information modernization and research programs, and develop a body of IW theory for China's unique situation. Training must be accelerated, and IW courses offered at institutions, key young people must be selected and provided with advanced training, and leaders and cadres in important posts must be systematically trained to increase their command abilities in an IW environment. Finally, the country must be aware that weapons with applied IT could become the means of exerting military, political and economic pressure on an enemy.[53]

Authors Wang Xusheng, Su Jinhai, and Zhang Hong of the PLA Academy of Electronic Technology listed the following as essential elements of IW theory and the latter's role in providing information security:

- primary goal is to attack command and control systems, the electronic solar plexus of the enemy
- fight with speed so that the enemy doesn't know where the actual battlefield is located
- attack command authorities, staff headquarters, theater of operations headquarters, and unit headquarters
- project force organization scenarios with increased roles for special small scale and flexible forces
- destroy enemy "eyes and ears" while protecting friendly systems

- use multi-node/path/frequency network systems equipped with information deception and concealment procedures to ensure survival
- use digitized equipment[54]

The foundation for IW is the network. The command network or nervous system has the following functions: gathering surveillance information, transmitting and processing information, locating targets, and allocating targets to be attacked, resulting in the categorization, collation, identification, and synthesis of information, thereby enabling precision attacks, transparency in command, and grasp of the initiative in war. IW is waged by all the people under high-tech conditions, and **electronics experts, computer experts, and information engineers are the new heroes on the stage of modern warfare**. Their basic need, Chinese experts assert, is the establishment of high-speed information networks. Mid and low speed networks exist, but additional ones are needed as well as the capability to do research on and build high speed ones. This will also require a variety of information resources and information equipment, systems, and qualified people to enable the country to achieve victory over an enemy without directly engaging him.[55]

To build an information-age China, the following plan was offered:

1. Build an information network architecture suitable for use by the civilian and military sectors in peacetime and wartime. IT not only has a multiplier effect on the growth of the national economy but also links the "market" with the "battlefield", in the opinion of the PLA Academy officers. The construction of an information superhighway with Chinese characteristics is essential.
2. Strengthen the training of qualified personnel. The **study of technology must be integrated with the creative innovation of military affairs theories**.
3. Networks must be created and free rein must be provided to the market's driving power, but government administration and coordinated development must be present as well to serve both the market and battlefield. China's Public Communications Network, Economic Information Network, and The China Education and Research Network (CERNET) are already taking shape.
4. New technology must be adopted quickly. The information environment is already being shaped by graphics, images, voice, and animations, made possible by surmounting some space and time limitations in technology. It also enables the battlefield to move from a passive to a dynamic environment.
5. The survivability of information networks must be enhanced. Otherwise, the orderly flow of personnel, material, energy resources and information will cease, and "soft kill" objects become unattainable. Flexibility, camouflage, and the ability to operate under a variety of conditions are most desirable. This requires the establishment of a military defense network.
6. Legislation concerning information and its administration must be strengthened. IT affects social, economic and cultural developments in many ways.[56] The Chinese officers feel that

> We should use legal mechanisms and norms to regulate, safeguard and guide the research, development and application of IT and information

> security technology. We should build a legal system of laws and regulations that standardizes, safeguards and promotes the application of IT. Thus the drafting, observance, and enforcement of laws relating to the application of IT will embody the objective laws of applied IT development, as well as embodying the role of IT in the context of the market economy, the national situation and the military situation.[57]

Views on Information War (1998)

Specific themes developed in 1998 include the requirement to develop a new strategy and tactics for waging a high-technology People's War; the need to integrate technology with theory while maintaining the most important elements of Chinese military history and philosophy; command and control issues; and the impact of information technology on military art.

Speaking at the Chinese National Defense University in January, Defense Minister Chi Haotian, a member of the Central Committee Political Bureau of the Communist Party of China (and Vice Chairman of the Central Military Commission) discussed the concept of People's War and its applicability to China today. His lecture, entitled "Issues Concerning the Modern High-Tech People's War," offered a systematic explanation of how to develop the concept of waging a high-tech People's War. Haotian stressed the fact that new focal points had appeared for accumulating the resources required to fight a People's War; and that new and effective means for mobilizing and inspiring the people to wage war against aggression had appeared. Since information technology is present in both the military and civilian sectors, there are now new methods for people to partake in and support a war, he added. These systems, which count heavily on integrated and rear support, offer new guidelines and measures for waging an extensive People's War. Strong reserve forces are needed, especially in terms of quantity, training, mobility, and equipment. People's War theories, strategies and tactics must be developed and enriched based on these new circumstances. Minds must be emancipated and mindsets changed in order to take advantage of this situation.[58] In particular

> we must focus on studying the characteristics and laws of fighting a People's War, building our defense, and waging high-tech military struggles; seize the commanding point of contemporary military theory; and actively create new strategies and tactics that meet the needs of waging a high-tech People's War.[59]

It will be interesting to follow the development of this theory and strategy over the next few years. It may offer a futuristic view of the total integration of the military and civilian sectors that all nations may someday employ.

A second issue receiving top priority in 1998 was the integration of technology with theory. This is an important topic to the Chinese, one which they will undoubtedly continue to develop over the next few years. They deem it absolutely invaluable to uncover the characteristics, objective laws, principles and stipulations associated with the ongoing RMA. Developing the theory of IW, in their view, is as important as the technology itself, since without it there is no means for the application of IT. In the realm of tactics, for example, the Chinese are investigating the objective laws of combined operations by studying the interaction between technology and tactics. This will improve the operational formulas and methodologies of the tactical and electronic means for the offense and defense and the art of command capabilities.[60] As one author noted

> in addition to the current three major factors of operations (firepower, assault, and mobility) the importance of protection, support, electromagnetic fighting, information and even command and control has attracted more and more attention. Obviously, people are giving play to the comprehensive effects of armaments and tactical means, emphasizing comprehensive and in-depth attacks at the same time, and increasing the percentage of technological confrontations in battle.[61]

The information age urges a new theoretical examination of the battlefield for several reasons. Now we are facing the nonlinearity of several issues: space (no regional boundaries), response (release combat power in unexpected places), coordination (different levels of command now must stay in contact), confrontation (operations are more asymmetrical than symmetrical), and decision-making (computers do non-sequential thinking).[62] The nonlinearity of these aspects invites a much closer examination than in the past.

Military theory itself also received attention. Some icons must be preserved, one analyst wrote, to wit Marxist military theory, Mao Zedong thinking on military affairs, Deng Xiaoping thinking on army building in the new period, and Chairman Jiang Zemin's important thoughts on army building. However, it is also important to emancipate the mind, boldly develop new theories, and study the impact of high-tech on the face of modern wars. Combat units will be employing advanced combat means and consuming a larger amount of resources on a multidimensional battlefield. Chinese officers must therefore study the military value of high-tech developments, understand the reason, purpose, scale, style, and means of high-tech warfare, analyze changes and characteristics of high-tech battlefields and combat methods, and identify the key factors concerning the process and outcome of high-tech wars. Otherwise it is not possible to properly prepare the force. The old adage of "one rifle, two legs, three meals, and four hand-grenades" must be replaced with "science, technology, system, quality, and efficiency."[63] Thinking outside the box will require breaking with old theories or reinterpreting them:

> Everyone is equal before truth; earnestly advocate creative and pioneering efforts; let a hundred flowers blossom and a hundred schools of thought contend; and weed through the old to bring forth the new...draw upon all advanced and beneficial military thinking; make foreign experiences serve China's purposes; and enrich and develop China's military theories.[64]

The Chinese explored other issues in 1998, especially the study of command and control issues. One report consisted of a book review in which the author noted that recent books on command and control warfare specified the following issues: the subject, object, means and other concepts of command and control; concepts for building an **information corps**; the principles on which information warfare should be based; and the means through which command and control should be exercised. The authors also examined the composition, characteristics and trends in the basic technologies of information warfare, its structural system, and the strategies for developing new technologies. Many of these questions will most likely be answered at the Communications Command Academy, an institution that combines command with technology and studies questions of organizational preparation and implementation of combat plans.[(65)]

One of the best general articles on IW in 1998 that expanded on ideas first developed in 1996 was that by Wang Jianghuai and Lin Dong called "Viewing Our Army's Quality Building from the Perspective of What Information Warfare Demands."[(66)] They discussed in detail several aspects of IW and its impact on military affairs. First, they noted, IW is the product of the new technological revolution, one that ensures that simply stronger firepower will not be enough to win in battle. Instead, who uses IW and IT to discover the enemy first, respond the fastest, and strike with accuracy will win. Effectiveness comes from the mastery of command and control capabilities, the ability to reduce interference in the decision-making process, and the introduction of interference into enemy systems or thinking. Second, information acquisition means will determine the accuracy of firepower and timeliness for the use of reserves. That is, accuracy comes from integrating means of reconnaissance and precision, and timeliness of the employment of forces also relies heavily on seeing the enemy first and anticipating his every move. The focus of operations will switch from firepower to detecting, concealing, searching and avoiding. Further, information now makes **non-contact engagements** as likely as contact engagements.

Third, the stability of the operational structure has become more important than the survivability of units. Traditional conflict witnessed the quantitative destruction of units (tanks, planes, etc.) to bring about structural disintegration. Now, the first efforts are aimed at command and control elements, for their destruction will destroy the utility and application of the units. Preserving the integrity and stability of the structure of one's own side and sabotaging the enemy's will be the **cornerstone of the operational theory of IW.** The overriding strike and long-range victory will advance to the forefront. The **principle of concentrating military strength will be replaced by that of concentrating operational effectiveness**. Since targets can be engaged literally hundreds of times, there will be a greater shock effect and explosive force with the effect of "nuclear fusion." With regard to the construction of the army, there will be a switch from functional expansion to structural optimization. Networked command that unites the various armed services will infiltrate to the tactical level.[(67)] Another author noted that the armed forces will be characterized by the downsizing of troops, improved quality and small, integrated and versatile units.[(68)] Fourth, the **core activity** is the pursuit of integrated information supremacy. Building systems of soft destruction (signal deception or interference) is more important than weapons of hard destruction. As system integration expands downward, it will integrate information, firepower, and mobility, and when it expands upward it will result in the infamous "system of systems."

The authors warn that IW is occurring in peacetime, reflected strategically as intelligence collection warfare and propaganda war. The superpowers are pushing the battle lines formed by information to the fore at the same time that they are pulling back regular forces. With the popularization of the Internet, this is becoming an affair of the whole nation. At the same time that China is presented with these challenges, there is also the golden opportunity to skip over several other phases of development in the mechanization process. This should be achieved not by buying equipment but by boosting domestic production capabilities.[(69)]

China's belief that preparations are ongoing for IW in peacetime puts added emphasis on preparations for and the necessity to win the initial battle, which they believe will develop into a decisive battle determining winners and losers. The core issue will be the battle for network supremacy, turning into a battle for the "nervous system" of the armed forces (remote sensing equipment, communications and transmission equipment, processing and decision-making nodes, etc.). As one author noted:

> the initial battle in future local wars may begin with a "hard" strike or may have "soft" strikes as its precursors. In addition, the causes of hi-tech local wars will be intricate and complex, involving not only the interests of neighboring countries but also directly or indirectly affecting the strategic interests of great powers and power blocs. The fact that policy and tactics play a major role in wars determines that it will not be possible to bring about and attain the objectives of war through traditional military means, and new means and forms of initial battles will emerge as the time requires.[70]

These new means and forms include political warfare, financial and economic warfare, psychological warfare, information network warfare, space control warfare, and regional blockade warfare. Initial battles may begin with "a keystroke" instead of a "first shot." The four most dangerous points of contention for this author were network early warning, space and air defense early warning, and early warning against an initial battle taking the form of a financial war. The recent Asian financial crisis served as a warning shot to the Chinese.[71] All of these issues are tied to networks, which will become the "commanding heights" for forces to capture.

On the battlefield, the authors suggest that China should focus on developing asymmetrical information offensive means. The use of physical symbols to transmit messages by Somalians, for example, crippled U.S. information gathering means, and should be remembered as a way of thinking asymmetrically. It is important to bring into play the mutual substitution and complementary use of both high and low technologies. China's force must focus on integration and the combination of four factors, opportunity, foundation, potential, and decision to determine the orientation, speed, and outcome of the armed forces' development.[72]

Finally, the Chinese offered an example of high-technology battlefield prowess in 1998 when it staged an integrated high-technology exercise in October that united several military regions around the country. The center of gravity of the exercise was the Beijing Military Region, where a joint defense warfare drill used a "military information superhighway" for the first time. It was described as an information network sub-system of the command automation system, composed of digital, dial, command net, and restricted channels. Other elements of the command automation system are the command operations, audio and graphics procession and control, and date encryption sub-systems. The exercise started on 20 October and was coordinated with several other regions. The superhighway transmitted graphics, characters, and audio data in addition to situation maps.[73] The Lanzhou Military Region, which includes the Gobi Desert, most likely also participated, since they reported on 26 October (as did the Beijing Region) of having participated in a high-technology exercise that emphasized electronic confrontation.[74] Earlier in October, the General Staff reported that it too had held an all-army high-technology training exercise to discuss and design training issues to meet the challenges of the worldwide military revolution. Fu Quanyou, chief of the General Staff, attended and presided over the training exercise. They viewed the training of the Shenyang Military Region,[75] which may also have been part of the exercise mentioned above.

Conclusions

There are many conclusions to be drawn from this short survey of Chinese writings on the RMA and IW over the past three years, but first it is worthwhile to summarize what was emphasized in each year. In 1996 Chinese specialists wrote on digitalization, the ability to inflict information injuries, using information to eliminate uncertainties, U.S. and other foreign army IW efforts, and the concept of a high-technology People's War. In 1997, an IW exercise was held, the idea of future war focused on the importance of high-technology "operational thinking" and "confrontation of commands," the concept of information security was developed, and a plan was offered to build an information-age China. In 1998, detailed discussions continued on a high-technology People's War, the impact of IW on military art, the essential requirement of integrating technology with theory (highlighting the role of networking and the initial period of war), and a major high-technology exercise was conducted (with the introduction of a "military information superhighway").

What conclusions can be drawn? First, these writings clearly were initially influenced by western perceptions and understanding of terms. Many of the definitions and characteristics associated with both RMA and IW drew heavily (in some cases entirely) on foreign army experiences. By 1997, however, it was also clear that the Chinese had arrived at a stage where they began to put their own spin and emphasis on the concepts. In particular, the Chinese began to stress asymmetrical and "out of the box" theoretical applications. Some of the terms highlighted above underscore this fact:

- take home battle
- network warriors/special warfare detachments
- invisible forces
- non-contact combat
- decision control war
- information injury
- guidance control injury
- negative entropy
- military soft science
- information corps
- and drift mobility

At the same time, Chinese theorists ensured that they did not eliminate the main elements of the Chinese understanding of warfare developed over thousands of years. Rather, the main lessons of past wars will be viewed through the prism of the current RMA and IW concepts. That is, Sun Tsu's Art of War and the 36 stratagems of military theory will now find new expression in RMA and IW theories.

Second, Chinese writings, similar again to western efforts, focused on the impact of the RMA and IW in three areas: weapons system integration, military theory, and military organization. Only when these three areas of analysis reach maturity will the Chinese feel they have arrived at a point where they are somewhat in control of the military revolution process. The Chinese look at the difficulties of the transition in terms of challenges and opportunities. Challenges are the problems associated with the proper integration of theory, weapons and organizational structure, while opportunities are the ability to skip some of the challenges presented by the mechanized age.

Third, the Chinese clearly have an optimistic attitude about the future. They do not look at the developments abroad as serious threats in the same manner that the Russians do, for example. Rather, they applaud creative efforts abroad and use them as examples for their people to follow, all the while emphasizing that one must learn from foreign armies but not copy their experience. Rather, the Chinese RMA and IW developmental phases must be full of unique Chinese characteristics and thinking.

Finally, it is clear that Chinese thinking stresses the increased role of the individual. The mere fact that a People's War has simply been reworked by Chinese theorists and adapted to the RMA and IW concepts is the best example of this fact. In addition, the Chinese stress the importance of people as the obvious "new heros" of the information age. In particular, they believe that the professions of electronics, computer, and information engineers will be just as vital in destroying an opponent's center of gravity as the infantryman. They may just be right.

On the other hand, access to the Internet has given the individual more power than ever before to reach other citizens and communicate throughout the mainland and the region. This has not been to the liking of the authorities. Neither has the rising number of hacker attempts on government websites, according to China's computer police. To counter this "information counterrevolution" the Ministry of Information Industry, which operates Internet servers for China, have created a so-called "Great Firewall of China" to keep out anything subversive.[(76)]

The difficulty for Chinese authorities will be to transition from a control-oriented information society to a computer dominated, open-information society. Russia is struggling with the same problem. The debate over access to information will be hotly contested over the coming months, as will information threats to the government. China is not immune from other information-oriented debates as well, such as developing a code of conduct for the information age or developing a region-wide information security system.

Above all, Chinese authorities do not believe that the development of an information society will solve societies problems. In the military sphere they correctly state, as have many American civilian and military think tanks, that IW will not be a panacea even for U.S. military strategists. LTG Li Jijun, Vice Chairman of the Chinese Institute of Military Sciences, noted that:

> this new military revolution is undoubtedly a new development, however, it will prove an ill omen to all countries, including the United States. The information age will make the most advanced country vulnerable to war damages, and to personnel casualties and network breakdowns in particular.[(77)]

Yet people and networks are the very areas over which China is most concerned, making it as vulnerable as any of the advanced countries of the world. Li Jijun's comment demonstrates that China will have much to work on to overcome its vulnerabilities. Internal conflict between the government and the people/businessmen over the right to use different forms of and access to information will be as contentious an issue as trying to compete with foreign militaries in the near future. The U.S. is still wrestling with this internal conflict of access to information as well. A recent court decision in the U.S. to allow access to pornography sites in high school libraries is a case in point. Most Americans would vehemently argue that access to this type of information in this particular environment is simply wrong, but the courts have ruled otherwise in the interim.

The primary area of concern for western governments will be Chinese intent, that is how they interpret what other nations are doing in this area and how they intend to respond with their own IW capability. It is important that governmental decisions about information operations in the U.S. and other western nations are clearly explained by diplomats and understood in China. To lessen concern on both continents, it would be beneficial to initiate high level discussions on this sensitive issue now. America is trying to do this with their Russian counterparts, and several important conferences have already been held. Leaders world-wide must confront this issue with the concern and patience it will require. We all must remain acutely aware of our shortcomings and take advantage of the time afforded us to discuss and solve these new, serious problems of the 21st century.

ENDNOTES

1. Wei Jincheng, "New Form of People's War," JIEFANGJUN BAO, 25 June 1996, p 6 as downloaded in translated form from the FBIS webpage.

2. Li Yinnian, quoted in column by Huang Youfu, Zhang Bibo, and Zhang Song, "New Subjects of Study Brought about by Information Warfare," JIEFANGJUN BAO, 11 November 1997, p 6 as translated on the FBIS web page, 23 December 1997.

3. Ch'en Huan, "The Third Military Revolution," Contemporary Military Affairs, 11 March 1996, as published in Michael Pillsbury, ed., Chinese Views of Future Warfare, National Defense University Press, 1996, pp 389-398.

4. Liang Zhenxing, (no title), presentation at the 15 September 1997 Defense Information Modernization Symposium organized by the Chinese Electronics Society, Zhongguo Dianzi Bao, 24 October 1997, from the FBIS web page of 13 January 1998.

5. Wang Baocun, "Military Transformation in an Information Era," Beijing Jiefangjun Bao, 21 April 1998, p 6 as translated and downloaded from the FBIS web page.

6. Definition obtained by the author during a recent trip to China.

7. Chinese Military Affairs Dictionary, Liberation Army Publishing House, 1990, p unknown, sent as an e-mail to the author after translation by James Mulvenon of the RAND corporation.

8. Hai Lung and Chang Feng, "Chinese Military Studies Information Warfare," Kuang Chiao Ching, No 280, 16 January 1996, pp. 22-23 as translated in FBIS-CHI-96-035, 21 February 1996, pp 33-34.

9. These have been defined as the calculation capacity of equipment, telecommunications volume, and the reliability and real-term reconnaissance ability of relevant systems.

10. Hai Lung, Ibid.

11. Zhang Feng, Historical Mission of Soldiers Straddling 21st Century," JIEFANGJUN BAO, 2 January 1996, p 6 as translated in FBIS-CHI-96-061, 28 March 1996, p 29.

12. Su Enze, "Have Mastery of Essence, Construct 'Two Mansions'," JIEFANGJUN BAO, 9 January 1996, p 6 as translated in FBIS-CHI-96-061, 28 March 1996, p 35.

13. Su Enze, "Logical Concept of Information Warfare," JIEFANGJUN BAO, 11 June 1996, p 6 as it appeared on the FBIS web page, 11 June 1996.

14. Cheng Yawen, "Keep Abreast of the Development Pattern of the New Military Revolution," JEFANGJUN BAO, 7 July 1998, p 6 as downloaded from the FBIS web page on 21 July 1998.

15. Baocun.

16. Ibid.

17. Yawen.

18. Ibid.

19. Zhang Feng, p 34.

20. Yang Shuqi and Guo Ruobing, (no Title), Beijing Zhongguo Guofang Keji Xinxi, Sept-Dec 1996, No 5/6, pp 90-93 as translated by FBIS and downloaded on its webpage.

21. Ibid.

22. Ibid.

23. Ibid.

24. Hai Lung and Chang Feng, "Chinese Military Studies Information Warfare," KUANG CHIAO CHING, 16 January 1996, no 280, pp 22-23, as translated and downloaded from the FBIS webpage.

25. Ibid.

26. Wang Baocun and Li Fei, "Information Warfare," in Chinese Views of Future Warfare, Michael Pillsbury, editor, National Defense University Press, Washington, D.C., 1997, p 328.

27. Shen Weiguang, "Focus of Contemporary World Military Revolution-Introduction to Research in Information Warfare," JIEFANGJUN BAO, 7 November 1995, p 6 as translated in FBIS-CHI-95-239, 13 December 1995, pp 23- 25.

28. Ibid., p 26.

29. Ibid., p 26, 27.

30. Ibid., p 28, 29.

31. These summaries of developments in each year are not claimed by the author to be all-inclusive, but represent only the general trends offered by translated material.

32. Zhang Feng, p 30.

33. Xue Lianfang, "Digitized Forces' Killer has Come into Being," JIEFANGJUN BAO, 30 April 1996, p 6, as translated in FBIS-CHI-96-097, 17 May 1996, p 24.

34. Wang Huying, "Exploring and Analyzing Characteristics of Information Warfare," JIEFANGJUN BAO, 30 January 1996, p 6 as translated and downloaded from the FBIS webpage.

35. Ibid.

36. Su Enze, "Have Mastery...", p 34.

37. Ch'en Huan, "The Third Military Revolution," Contemporary Military Affairs, 11 March 1996, as published in Michael Pillsbury, ed., Chinese Views of Future Warfare, National Defense University Press, 1996, pp 389-398.

38. Wei Jincheng.

39. JIEFANGJUN BAO, 25 June 1996, p 6 as translated in FBIS-CHI-96-145, 26 July 1996, pp 27, 28.

40. Zhang Feng, p 33, 34.

41. Liang Zhenxing.

42. Beijing Xinhua, 1508 GMT, 22 October 1997, as downloaded in translated form from the FBIS webpage.

43. Taiwan Central News, 1057 GMT, 27 December 1997, as downloaded in translated form from the FBIS webpage.

44. Liang Zhenxing, (no title), Zhongguo Dianzi Bao, 24 October 1997, as translated and downloaded from the FBIS webpage.

45. Ibid.

46. Ibid.

47. Ibid.

48. Ibid.

49. Ibid.

50. Xu Runjun and Chen Xinzhong, "Computer Virus Weapons," GUOFANG, 15 February 1997, No 2, pp 42-44, as translated and published on the FBIS webpage.

51. Ibid.

52. Ibid.

53. Li Nengjing, (no title), Zhongguo Dianzi Bao, 24 October 1997, p 8, as translated and downloaded on the FBIS webpage.

54. Wang Xusheng, Su Jinhai, and Zhang Hong, (no title) Beijing Jisuanji Shijie, 11 August 1997, No 30, as translated and downloaded on the FBIS webpage.

55. Ibid.

56. Ibid.

57. Ibid.

58. Beijing Xinhua Domestic Service, 0921 GMT 8 January 1998, as translated and downloaded from the FBIS web page.

59. Ibid.

60. Zeng Sunan, "New Technological Revolution Calls for Breakthrough in Military Theory," Hong Kong Hsien-tai Chun-shih, No 259, 11 August 1998, p 19-20, as translated and downloaded from the FBIS web page.

61. Ibid.

62. Guo Anhua and Zhang Haitian, "Increase Sense of Times, Vigorously Explore Laws," Beijing Jiefangjun Bao, 21 July 1998, p 6 as translated and downloaded from the FBIS web page.

63. Fu Quanyou, "Study Military Theories, Proper Military Science," Beijing Jiefangjun Bao, 10 March 1998, p 6 as translated and downloaded from the FBIS webpage.

64. Ibid.

65. Lei Yuanshen, "New Breakthrough in the Study of Information Warfare," Beijing Jiefangjun Bao, 21 July 1998, p 6 as translated and downloaded from the FBIS webpage.

66. Wang Jianghuai and Lin Dong, "Viewing Our Army's quality Building from the Perspective of What Information Warfare Demands," Beijing Jiefangjun Bao, 3 March 1998 p 6 as translated and downloaded from the FBIS web page.

67. Ibid.

68. Baocun. In the reform process, Baocun notes that the army will most likely follow a "comprehensive" development, meaning the army will be ready for both mechanized and information warfare.

69. Jianghuai and Dong.

70. Zhao Shuanlong, "The Initial Battle is the Decisive Battle, and Preparations for Military Struggle in the New Period," Beijing Jiefangjun Bao, 18 August 1998, p 6 as translated and downloaded from the FBIS web page.

71. Ibid.

72. Jianghuai and Dong.

73. Beijing Xinhua Domestic Service, 1148 GMT, 26 October 1998, as translated and downloaded from the FBIS web page.

74. Ren Yanjun and Zhang Jianjun, "General Staff Department Holds All-Army Hi-Tech Training Exercise," Beijing Jiefangjun Bao, 2 October 1998, p 1 as translated and downloaded from the FBIS web page.

75. Beijing Zhongguo Xinwen She, 1309 GMT, 26 October 1998, as translated and downloaded from the FBIS web page.

76. Elaine Kurtenback, "China Determined to Tighten Secrecy," Associated Press, 25 November 1998.

77. Li Jijun, "International Military Strategy and China's Security at the Turn of the Century," Hong Kong Zhongguo Pinglun, No 8, 5 August 1998, pp 76-80 as translated and downloaded from the FBIS web page.