Information Warfare : The Latest Chinese Thrust Area

Major General SV Thapliyal, SM (Retd)

Introduction

Perhaps the most profound transformation to take place in the PLA Army has been the wide and deep application of information technology to enable the development of joint doctrine and tactics, to increase the ability of PLA Army to surveil and target its enemies, and to give its weapon systems more combat power. The PLA has given this broad doctrinal aspiration the term "informationalisation." To be sure, the PLA has been able to pursue this aspiration largely as China has developed a modern information sector to include building a substantial national fibre optics network and a world class computer and electronics sector. This process has been assisted by a very broad commercial interaction with companies in the USA, Japan and Europe.

Each PLA Military Region now has a "Special Technical Reconnaissance Unit" which is responsible for mainly computer network attack "information warfare" and its members are often reservists drawn from the civilian computer sector. But the PLA has also closely followed the US Military experience as the world leader in developing military information innovations. One can see widespread use of wireless laptops throughout the PLA services.[1]

In addition, the PLA has also sought specific foreign information technologies to enhance its combat power. It has obtained Russian electro optical and radar satellite technology, and French communication satellite technology. Russian and Ukrainian naval radar technology dominates new PLA warships. Russians have accused the Chinese of stealing their application of modern computer processing to produce better counter stealth

*Major General SV Thapliyal, SM (Retd) was commissioned into Regiment of Artillery on 25 Dec 1966. After premature retirement from the Army in May 2004, he completed his PhD on Sino-Indian relations. Presently, he is Vice President of a multinational IT company.

radar. China is also producing its own passive radar, patterned after the innovative Ukrainian Kolchuga radar, which is also an excellent counter stealth system. While the Israeli Phalcon aerial active phased array radar (APAR) was supposed to have been denied to China in 2000, a radar with similar characteristics is now flying on three AWACS aircraft. The PLA is developing APAR technology into a long range electronic attack weapon, by using the array to focus radiated energy on target electronic systems.

Information Warfare (IW) with Chinese Characteristics[2]

How has the information age affected China's attitude toward warfare? It is fair to say that the major change was a re-evaluation of how to evaluate and conduct warfare. China realised that it couldn't threaten countries as a superpower might do with its current nuclear force, but something it can do with its IW force. For example, China can theoretically threaten the US financial stability through peacetime IW. Electrons lie at the heart of not only IW but also with worldwide economic boom associated with stock markets and e-commerce. The characteristics of information (global reach, speed of light transmission, non-linear effects, inexhaustibility, multiple access, etc.) control the material and energy of warfare in a way that nuclear weapons cannot. IW attempts to beat the enemy in terms of promptness, correctness, and sustainability, and electrons are capable of reaching out and touching someone a long way away. It thus makes complete sense to put a significant effort into developing an information-based capability in both the civilian and military sense. From the Chinese point of view, IW is like adding wings to a tiger, making the latter more combat worthy than ever before.

Recent reports of hacker attacks indicate that China is moving from theory to practice in security matters as well. The Washington Times reported that hackers suspected of working for a Chinese government institute broke into a Los Alamos computer system and took large amounts of sensitive but unclassified information. Los Alamos spokesman Jim Danneskiold stated that "an enormous amount of Chinese activity hitting our green, open sites" occurs continuously. India's National Security Adviser also reported attempt by Chinese to hack into PMO computers.

Targets of Chinese IW include information sources, channels, and destinations, and C4I and electronic warfare assets. First attack objectives, some note, will be the computer networking system linking political, economic and military installations of a country as well as society in general; and the ability to control decision-making to hinder coordinated actions. This requires that both cognitive and information systems are hit. This IW focus implies that not just soldiers will conduct warfare in the future, but civilians too. Some Chinese theorists have recommended organising network special warfare detachments and computer experts to form a shock brigade of 'network warriors' to accomplish this task. They will look for critical nodes and control centres on networks, and sabotage them. Thus both computer experts and soldiers, a reflection of China's changing attitude, may conduct warfare.

A senior official on the PLA General Staff has declared, "The twenty-first century will be an information era, and wars in the twenty-first century will be information wars. We can say that whoever has the advantage of information and the control of information will have the initiative and will win future wars". "Which are more powerful?" ask Chinese experts-nuclear or information weapons? They answer that this is a difficult question since it resembles "a contest between a lion and a tiger."

According to Major General Wang Pufeng, former head of China's Academy of Military Science, IW refers to a kind of operation and a kind of operational pattern. Along with changes in the war pattern in the current information era, IW has already become a major pattern for high-tech operations. The PLA must shift its concept from waging electronic warfare-which is but a prelude to IW to fighting IW, and from seizing the electromagnetic initiative to seizing the information initiative.

Major General Xu Xiaoyan[3], Director of the General Staff's Communications Department, has outlined seven strategies to implement "leaps" in technical development based on information technologies. These are :-

(a) **Embeded transformation.** Implant or merge advanced information technologies into equipment already in service; thereby, achieving the lead in combat effectiveness.

(b) **Integrate systems.** Take existing, separate, loosely connected, or unconnected subsystems and merge them to form a new integrated and tightly connected system.

(c) **Direct upward leaps.** Conduct research, development, testing and evaluation directly in accordance with informationisation standards, in order to leap over the mechanisation phase and proceed directly to informationisation.

(d) **Borrow/import.** Absorb advanced technologies and products used in foreign militaries in accordance with the overall requirements of the PLA's informationisation effort; thereby, increasing the speed and effectiveness of military development.

(e) **Rely on compatibility.** Exploit the dual-use nature of information technology, using the combination of military and civilian technologies as the main measuring rod.

(f) **Upgrade structure.** Exploit the characteristics of information technology as a multiplier, thereby reforming, adjusting, optimising, and upgrading military structures through the enhancement of information capabilities.

(g) **Innovate measures.** Increase the speed of military development by incorporating innovative scientific research methods.

According to Chinese military scientists, information weapons may be roughly divided into three types : weapons that destroy the enemy's national defence, state and economic infrastructures; psychological weapons; and weapons that use wireless suppression procedures. Targets of the first type include the enemy's national defence information systems, telecommunications systems, electric power distribution systems, petroleum and natural gas storage and transportation systems, banking and finance systems, transportation systems, water supply systems, emergency services systems, etc. The target is not merely the information system itself; an even greater emphasis is placed on using new technologies to alter informational content without otherwise affecting the information carrier. Targets of psychological weapons include both operating personnel and civilians. Finally, weapons that use wireless suppression procedures emit or reflect electromagnetic waves, sound waves or infrared signals, etc., that can knock out the enemy's electrical equipment, sonar or infrared equipment.

Chinese military scientists assert that future wars may become too "civilised" and that a smokeless computer war is likely to achieve combat objectives through "soft casualties." Tactics in this kind of warfare might include electromagnetic field probing and advance, timely and indirect planting of computer viruses.

Information Weapons/Operations

"New-concept" weapons,[4] say the Chinese, are completely new information weapons that use advanced technologies (especially information technology) and new casualty-and-damage-producing mechanisms. Major weapons of this type include : super-kinetic energy weapons (electromagnetic guns), directed-energy weapons, artificial intelligence weapons, thought control weapons and micro-electromechanical weapons (miniature robotic electronic incapacitating weapons).

Information Warfare[5] – said to be the dialectical counter to PGMs – is conducted in six-dimensional strategic space : ground, sea, air, space, information and cogitation. Major General Dai Qingmin – Director of the General Staff's Fourth Department and the PLA's "senior electronic warfare official" – has provided a series of guidelines that serve as a theoretical foundation for conducting information operations. The guidelines include suggestions for integrating operations, adopting multiple means, and focussing on strategies. In integrating operations, he stresses : the integrated use of IW forces, both military/civilian and professional/non-professional; the integrated application of IW assets – both network space and electromagnetic space as well as "soft" and "hard" weapons; and the integration of offensive and defensive operations as well as all-dimensional operations. Adopting multilple means by launching an attack on the enemy's CISR system in all-dimensional space simultaneously or one after another, he says, is the only way for the inferior side to be able to conduct effective information operations and seize local information control. The guidelines focus on strategies, meanwhile, as a critical factor in defeating superior forces with inferior ones in future information operations. While an army with high-tech superiority may overwhelm an enemy with accurate or highly mobile assault arms, it will have to rely on advanced – but exceedingly vulnerable – CISR systems.

Dai has also provided the theory behind “integrated network – electronic warfare. “The ideology” of integrated network – electronic warfare represents “a total innovation in information operations theory.” It embodies information operations theory with Chinese characteristics – a synthesis of foreign and uniquely Chinese military – theoretical achievements. Integrated network – electronic warfare has the following four main characteristics :

(a) **Comprehensive Combat Objectives.** In future high-tech warfare, the destruction and control of the enemy’s information infrastructure and strategic lifeblood-by selecting key targets and launching effective network-electronic attacks-can directly constrain the enemy’s strategic planning. It can weaken and even paralyse his overall combat potential-including political, economic and military aspects. Integrated network-electronic attacks thus have a comprehensive effect on the enemy.

(b) **Integrated Methods of Combat Operations.** Weakening and destroying the overall effectiveness of the enemy’s information systems while protecting one’s own is a joint objective in both network and electronic warfare. Therefore, when executing an information attack, the PLA must have a unified plan and organisation for both, so that they will be coordinated closely, become a single entity and constitute an integrated attack against a single target. When executing information defence, network and electronic defence must similarly be incorporated into a unified system with an integrated plan and coordinated execution.

(c) **An Expansive Battlespace.** The integrated employment of network and electronic warfare transcends the traditional boundaries of network space and the domain of the electromagnetic spectrum. Full-depth integrated attacks, non-contact combat operations, non-linear combat operations, etc., will permeate the entire course of combat on the informationised battlefield. Integrated network-electronic warfare will be conducted in a battlespace larger than that of any current form of warfare.

(d) Integrated Operational Effectiveness. Integrated network-electronic warfare selects as its main targets of attack the normal operation of information systems in the enemy's military, political, economic and social systems. It seeks to cut these nerves and paralyse the entire body. Therefore, the combat effect resulting from such warfare exceeds that of any traditional or single form of combat operations.

Since Operation Iraqi Freedom, Major General Dai Qingmin[6] has asserted that conducting information-based warfare requires the following four basic capabilities :-

(a) Integrated Information Support Ability. The high-level combination of all-dimensional information perception, real-time information transmission, intellectual information disposal forms, integrated information support ability, and becomes "the base and the backbone" of China's information-based warfare system.

(b) Information-Based Fire Strike Ability. Information technology has propelled the Chinese transformation from mechanised firepower to information-based firepower. Information-based weaponry and equipment tend to be developed in the direction of being accurate, miniature, stealthy and unmanned.

(c) Multi-Level Information Warfare Ability. China's ability to totally destroy the enemy's information-based warfare system-the essence of IW depends on whether China's IW system can develop multi-level and all-directional IW capabilities.

(d) All-Directional Comprehensive Protective Ability. China's integrated protective system requires efforts to improve the "Three-Counterattack and One Resistance" abilities of the information system.

Conclusion

The PLA considers active offensive operations to be the most important requirement for information warfare to destroy or disrupt an adversary's capability to receive and process data. Launched mainly by remote combat and covert methods, the PLA could employ information warfare pre-emptively to gain the initiative in a crisis. Specified information warfare objectives include the targeting the destruction of an enemy's command system, shortening the duration of war, minimising casualties on both sides, enhancing operational efficiency, reducing effects on domestic populations and gaining support from the international community. The PLA Army's IW practices also reflect investment in electronic countermeasures and defence against electronic attack (e.g. electronic and infrared decoys, angle reflectors and false target generators).

China's computer network operations (CNO) include computer network attack, computer network defence 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, 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.

End Notes

1. China's New Great Leap Forward – High Technology and Military Power in the Next Half Century – Hudson Institute Report.

2. China's High Technology Development : US-China Economic and Security Review Commission – 21 April 2009 by Kathleen Walsh.

3. CIA's Annual Report to US Congress 2009 – Military Power of the People's Republic of China.

4. Report on China's Science and Technology System, EST Section of the US Embassy in Beijing, October 2008.

5. Hearing on China's High Technology Development. US-China Economic and Security Review Commission April 2009 by Dr. Denis Fred Simor, USA.

6. The Impact of Technology on the Modernisation of Chinese People's Liberation Army. A Report on the US-China Economic and Security Review Commission, January 2008 by Richard D. Fisher Jr.