China's Emerging Cyber War Doctrine

*Gurmeet Kanwal**

China will develop much greater depth and sophistication in its understanding and handling of information warfare techniques and operations. With Indian security becoming increasingly dependent on date processing and network centricity, it will become extremely vulnerable to such information warfare campaigns. India needs to adopt a multi-disciplinary approach towards dealing with the emerging cyber warfare threats and develop appropriate response. Since no single agency is charged with ensuring cyber security, there is a need to create a lead agency under a national cyber security advisor to spearhead the counter cyber war efforts. The military, too, needs to form an important part of the overall national effort. Raising of a military cyber command may, therefore, be in order.

On June 23, 2009, Robert Gates, the United States (US) Secretary of Defence, authorised the creation of a new military command that will develop offensive cyber-weapons and defend command and control networks against computer attacks.

In alarming front page news reports published by several Indian newspapers recently, Chinese cyber spies were reported to have hacked into computers and stolen documents from hundreds of government and private offices around the world, including those of the Indian embassy in the US. Earlier it had been reported that the Chinese army uses more than 10,000 cyber warriors with degrees in information technology to maintain an e-vigil on China's borders. "Chinese soldiers now swipe cards and work on laptops as they monitor the border with great efficiency with electronic sentinels functioning 24 hours a day."

While information about the People's Liberation Army's (PLA) cyber warriors has begun to appear in the public domain only recently, PLA watchers across the world have known for long about China's well conceived doctrine on information operations and cyber war. China's cyber war doctrine is

With electronic sentinels, Chinese soldiers now monitor the border 24 hours a day.

* Brig. Gurmeet Kanwal (Retd.) is Director at Centre for Land Warfare Studies, New Delhi.

designed to level the playing field in a future war with better-equipped Western armed forces that rely on Revolution in Military Affairs (RMA) technologies and enjoy immense superiority in terms of weapons platforms and intelligence, surveillance and reconnaissance (ISR) and command and control networks.

Informationisation

Early in the first decade of the new century, the Central Military Commission (CMC) called for a detailed study of the concept of people's war under conditions of 'informationisation.' Describing the new concept, Ka Po Ng, an associate professor at Aichi Bunkyo University, Japan, has written,[1] "...what the PLA is prepared to fight is a people's war in the form of a 'local war under high-tech conditions' with increasing attention to the application of information technology." Since then China has spent a lot of time and effort in assessing the implications of information technology and knowledge-based warfare on the modern battlefield and to applying the lessons to its own war concepts. Parallel to this effort, China is also engaged in raising a private army of hackers who will wage cyber war against the state's enemies from their laptops at home.

PLA persists in taking mechanisation as the base to promote informationalisation and informationalisation as the driving force to bring forward mechanisation.

The PLA expects to fight the next war under conditions of what it calls 'informationisation' or 'informationalisation.'[2] In the White Paper on National Defence issued in 2004, informationisation was explained only in general terms, but bears repeating: "To adapt itself to the changes both in the international strategic situation and the national security environment and rise to the challenges presented by the RMA worldwide, China adheres to the military strategy of active defence and works to speed up the RMA with Chinese characteristics:[3]

To Take the Road of Composite and Leapfrog Development: Going with the tide of the world's military development and moving along the direction of informationalisation in the process of modernisation, the People's Liberation Army (PLA) shall gradually achieve the transition from mechanisation and semi-mechanisation to informationalisation. Based on China's national conditions and the PLA's own conditions, the PLA persists in taking mechanisation as the foundation to promote informationalisation, and informationalisation as the driving force to bring forward mechanisation. The PLA will promote coordinated development of firepower, mobility and information capability, enhance the development of its operational strength

with priority given to the Navy, Air Force and Second Artillery Force, and strengthen its comprehensive deterrence and war-fighting capabilities.

PLA persists in taking mechanisation as the base to promote informationalisation and informationalisation as the driving force to bring forward mechanisation

To Build a Strong Military by Means of Science and Technology: The PLA works to improve its combat capabilities by taking advantage of scientific and technological advances and aims at building qualitative efficiency instead of a mere quantitative scale, and transforming the military from a manpower-intensive one to a technology-intensive one. Implementing the Strategic Project for Talented People, the PLA focuses on training a new type of high-calibre military personnel.

To Deepen the Reform of the Armed Forces: Based on the transformation of modern warfare and the requirements of the socialist market economy, the PLA seeks to achieve development and breakthroughs in the process of reform and innovation. The PLA develops its military theories in an innovative spirit, and explores the laws of building the army and conducting operations under the condition of informationalisation.

To Step Up Preparations for Military Struggle: The PLA takes as its objective to win local wars under the conditions of informationalisation and gives priority to developing weaponry and equipment, to building joint operational capabilities and to making full preparations in the battlefields.

Informationalisation relates to the PLA's ability to adopt information technologies to command, intelligence, training and weapon systems.

PLA analysts have called the ongoing RMA an "informationised military revolution".[4] It emerges that informationisation "clearly relates to the PLA's ability to adopt information technologies to command, intelligence, training and weapon systems. This would include broad investment in new automatic command systems linked by fibre-optic Internet, satellite and new high-frequency digital radio systems. The PLA can also contest the information battle space with its new space-based, airborne, naval and ground-based surveillance and intelligence gathering systems and its new anti-satellite, anti-radar, electronic warfare and information warfare systems. There is increasing 'information content' for new PLA weapons as it moves to link new space, airborne and ELINT sensors to missile, air, naval and ground-based 'shooters' to enable all its services to better use new precision-strike weapons."[5] According to the 2004 White Paper, "In its modernisation drive, the PLA takes informationalisation as

Basic PLA Doctrine of Local Wars under Hi-tech Conditions

Underpinning the new professionalism of the PLA is the basic doctrine of 'active defence' (jiji fangyu) that seeks to conduct 'people's war under modern conditions' (better understood as 'local wars under hi-tech conditions'—gaojishu tiaojian xia de jubu zhanzheng). The 'active defence' doctrine calls for integrated, deep strikes - a concentration of superior firepower that is to be utilised to destroy the opponent's retaliatory capabilities through pre-emptive strikes employing long-range artillery, short-range ballistic missiles (SRBMs) and precision guided munitions. The new doctrine and the strategy and tactics associated with it have been influenced by the lessons of Gulf War I in 1991 and the Iraq War of 2003, both of which have been extensively studied by Chinese scholars. The doctrine requires the creation of a capability to project force across China's borders through rapid deployment, conventional SRBMs and cruise missiles, information warfare, electronic warfare, precision-guided munitions, night fighting capabilities and other advanced military technologies. Beijing has defined the following five as likely limited war scenarios: military conflict with neighbouring countries in a limited region; military conflict on territorial waters; undeclared air attack by enemy countries; territorial defence in a limited military operation; and punitive offensive with a minor incursion into a neighbouring country.

its orientation and strategic focus." The PLA has adopted what it calls a "double historical mission" and a "leapfrog development strategy" – accelerating military informationisation while undergoing mechanisation.[6]

Information Operations – Acupuncture Warfare

The denial of information, strategic deception and the achievement of psychological surprise have for long been an integral part of Chinese military doctrine. The Chinese find Information Warfare (IW) extremely attractive as they view it as an asymmetric tool that will enable them to overcome their relative backwardness in military hardware. The Chinese are devoting considerable time and energy to perfecting the techniques of IW to target the rapidly modernising Western armed forces that are becoming increasingly more dependent on the software that runs computer networks and modern communications. In Chinese thinking, IW presents a level playing field for projecting power and

> In China, IW presents projecting power and prevailing upon the adversary in future wars.

prevailing upon the adversary in future wars. However, it has not been possible to ascertain from open public sources whether IW is fully integrated with the doctrine of people's war under modern conditions or if it is still treated as a separate but complementary pattern of war (zhanzheng xingtai). There is also some confusion created by the use of the term 'informationised warfare' (xinxihua zhanzheng) instead of IW (xinxi zhanzheng).[7] However, there is no ambiguity in the manner in which the Chinese view information operations:[8]

- Intelligence operations, which include intelligence reconnaissance and protection.
- Command and control operations to disrupt enemy information flow and weaken his C2 capability while protecting one's own.
- Electronic warfare by seizing the electromagnetic initiative through electronic attack, electronic protection and electronic warfare support.
- Targeting enemy computer systems and networks to damage and destroy critical machines, networks and the data stored on them.
- Physical destruction of enemy sources like information infrastructure such as C4ISR through the application of firepower.

The Chinese call their pursuit of information warfare and other hi-tech means to counter Washington's overwhelmingly superior conventional military capabilities 'acupuncture warfare', a term that first surfaced in a 1997 PLA National Defence University publication entitled "On Commanding Warfighting under High-Tech Conditions."[9] Acupuncture warfare (also called 'paralysis warfare'[10]) was described as 'Paralysing the enemy by attacking the weak link of his command, control, communications and information as if hitting his acupuncture point in kung fu combat.' Acupuncture warfare is a form of asymmetrical warfare dating back to the teachings of Sun Tzu, China's pre-eminent military strategist from the fifth century BC. For quite some time now, the PLA has been simulating computer virus attacks in its military exercises.

Paralysing the enemy by attacking the weak link of his command, communications and information is hitting his acupuncture point in *kung fu* combat.

According to a US Congressional Research Service report entitled 'Cyberwarfare', authored by Steve Hildreth, China is developing a strategic information warfare unit called 'Net Force' to neutralise the military capabilities of technologically superior adversaries.[11] This new information

warfare unit will “wage combat through computer networks to manipulate enemy information systems spanning spare parts deliveries to fire control and guidance systems.” Though the PLA's research into the theoretical aspects of information warfare is fairly advanced, it does not appear to have developed a coordinated and integrated information warfare doctrine as yet.

Chong-Pin Lee, Vice Chairman of Taiwan's Mainland Affairs Council, says Beijing is re-directing its emphasis away from nuclear deterrence to this new asymmetrical strategy and its “overarching purpose is to deter the United States from intervening around China's peripheries and to seize Taiwan with minimum bloodshed and destruction.”[12] In another five to ten years, China will develop depth and sophistication in its understanding and handling of information warfare techniques and information operations. With Indian society becoming increasingly dependent on automated data processing and vast computer networks, India will also become extremely vulnerable to such information warfare techniques. The fact that it can be practiced from virtually any place on the earth even during peacetime makes acupuncture warfare even more diabolical. India can ill-afford to ignore this new challenge to its security.

Defence analysts, Timperlake and Triplett have written that economic, political and social systems are essentially unprotected against Chinese information warfare attack. In their view, China has adopted a comprehensive strategy to further its information warfare plans,[13] Information warfare has the support of the top PLA brass; the PLA's best strategists and defence scientists have had extensive open discussions about information warfare; the PLA is conducting military exercises in information warfare; it is expanding its already strong signals intelligence (SIGINT) capability in Cuba; and the PLA is buying the hardware necessary. As supercomputers require huge capital investments, a strong political and financial commitment is implied. The Chinese are recruiting scientists and technicians and are building related weapons such as high-powered microwave weapons.

The PLA is acutely conscious of its continuing relative backwardness in information technologies. To prepare itself for a conflict with an RMA-ready opponent, China's military thinkers recommend that China must,[14] 'Close the information gap; network all forces; attack the enemy's C3I to paralyse it; use directed energy weapons; and computer viruses.' Physical measures include the use of submarine-launched munitions; anti-satellite weapons; forces to prevent a logistics build-up and special operations raids. Timothy Thomas, of the Foreign Military Studies Office at Fort Leavenworth, has written about a 1999 'network battle' fought between Chinese and American “hackers after the US bombed the Chinese embassy in Belgrade.”[15]

In fact, efforts to inculcate an IT culture are being extended all the way down to the troops deployed to guard to China's borders,[16] “With a vast pool of IT-trained officers in place, China's border vigil is turning electronic. At its long

border with 14 countries, including India, the Chinese soldiers now swipe cards and work on laptops as they monitor the border with great efficiency with electronic sentinels functioning 24 hours a day along the sea and land boundaries while sentries work with IC cards and other sophisticated equipment. The use of electronic devices has enhanced the army's ability to deal with emergencies quickly and efficiently, according to sources."

Cyber Warfare

Developing cyber warfare capabilities is seen as presenting a level playing field in an otherwise David versus Goliath scenario, as Chinese hardware is no match for the weapons technology fielded today by the US and its allies. Recent cyber attacks directed against Taiwan and the US are indicative of the efforts to develop new techniques, viruses and logic bombs. Information Warfare will be crucial in the opening phases of a war aimed at the re-unification of Taiwan or a border conflict with India as it will be important to knock out the adversary's communications infrastructure by cyber as well as physical means. A private army of young civilian hackers on whom the state can bank during crises is being developed for this purpose besides the employment of regular PLA personnel.[17]

Compared with China's historically reactive stance of luring the enemy in deep and destroying him through strategic defence, the present doctrine is essentially proactive and seeks to take the battle into enemy territory. It also strives to achieve surprise in a proactive manner that is demonstrated by new 'quick-strike' tactics. The aim is to catch the enemy unprepared in order to inflict substantial damage on strategic targets and disrupt logistics to gain psychological ascendancy. While the land frontier is expected to continue to generate some local tensions, the CMC has identified space and the oceans as the new areas where future conflict might take place.

Besides the employment of regular PLA personnel, a private army of young civilian hackers are being developed.

The Chinese have rejected the doctrine of deterrence as, in their view, it is associated with imperialism, amounts to military blackmail, glorifies the use of force and would be an empty threat if not substantiated by tangible power.[18] The 'active defence' doctrine also calls for integrated deep strikes—a concentration of superior firepower that is to be utilised to destroy the opponent's retaliatory capabilities by employing long-range artillery, short-range ballistic missiles (SRBMs) and precision guided munitions. The doctrine emphasises the effective use of advanced equipment wielded by elite units, with a focus on joint operations. The overall aim in this 'limited war under hi-tech conditions' doctrine is to cause heavy attrition and

disrupt the enemy's combat forces and logistics so as to bring about a negotiated end to the conflict or dictate terms if possible.

The Chinese have rejected the doctrine of deterrence as it is associated with imperealism, amounts to military blackmail and would be an empty threat if not substantiated by tangible power.

Concluding Observations

In another five to ten years, China will develop much greater depth and sophistication in its understanding and handling of Information Warfare techniques and information operations. With Indian society becoming increasingly dependent on automated data processing and vast computer networks, India will also become extremely vulnerable to such information warfare techniques. The fact that it can be practiced from virtually any place on the earth even during peacetime makes acupuncture or paralysis warfare even more diabolical. India can ill-afford to ignore this new challenge to its security.

India should adopt an inter-ministerial, inter-departmental, inter-Services, multi-agency approach to dealing with emerging cyber warfare threats and must develop appropriate responses. No single agency in India is charged with ensuring cyber and IT security. A nodal agency must be created to spearhead India's cyber war efforts under a national cyber security advisor who should report directly to the NSA. The armed forces must be part of the overall national effort from the very beginning so that emerging tactics, techniques and procedures can be incorporated into doctrine and training. Hence, India too needs a Cyber Command to lead efforts within the military to safeguard computer networks from hackers and cyber attacks.

The strategy must be defensive to guard India's vulnerable assets, such as military command and control networks and civilian infrastructure dependent on the use of cyber space, as well as offensive to disrupt the adversary's C4I2SR systems and develop leverages that can be exploited at the appropriate time. With some of the finest software brains in the world available to India, it should not prove to be an insurmountable challenge.

This is too important a field to allow the traditional Indian approach – digging heads into the sand while waiting for the threat to go away – to hold sway and react only when the enemy has reached Panipat and is knocking on the gates of Delhi. In this case, the nothingness of cyberspace connects China's laptops warriors directly with Delhi, Mumbai, Kolkata, Chennai, Bangalore and Hyderabad and other Indian cities, as also India's strategic establishments.

Notes

1. Ka Po Ng, "Interpreting China's Military Power: Doctrine Makes Readiness", Abingdon, Oxon: Frank Cass, 2005, pp. 21.
2. Western governments and analysts are using both the terms 'informationisation' and 'informationalisation' interchangeably. It has not been possible to get an exact equivalent to the corresponding Chinese phrase from an authoritative source. From the point of view of language aesthetics and phonetics, the term informationisation is preferred here. It is also to be noted that the Chinese themselves now increasingly prefer the term informationisation in their writings.
3. "China's National Defence in 2004", White Paper on National Defence published by the Government of the People's Republic of China.
4. Zhou Fangyin, "The Impact of Information Revolution upon Military Affairs and Security", Contemporary International Relations, 7 (2001), pp. 28.
5. Testimony of Richard D. Fisher Jr., "China's Military Power: An Assessment from Open Sources", International Assessment and Strategy Centre, before the Armed Services Committee of the US House of Representatives, July 27, 2005, at www.strategycenter.net.
6. Ka Po Ng, "Interpreting China's Military Power: Doctrine Makes Readiness", Abingdon, Oxon: Frank Cass, 2005, pp. 109.
7. Ibid.
8. Ibid.
9. Barbara Opall-Rome, "PLA Pursues Acupuncture Warfare", Defense News, Springfield, Virginia, USA, March 1, 1999.
10. "According to the Taiwanese Ministry of National Defence, China is shifting from deterrence-based strategy to pre-emptive strike strategy... 'Paralysis warfare features web-based information warfare, saturation ballistic missile attacks, joint precision strikes and seizure of the enemy's capital city by special operation units... Such tactics will become major options for the Chinese military in its choice of modes of modes of attack..." Srikanth Kondapalli, "A Great Leap Forward Modernization: China's Armed Forces in 2003", Centre for China Studies, National Chengchi University, Taiwan, 2005, pp. 27, cited from Brian Hsu, "China Developing 'Paralysis Warfare", Taipei Times, October 8, 2003, FBIS-CHI-2003-1008, October 10, 2003.
11. Jason Sherman, "Report: China Developing Force to Tackle Information Warfare", Defense News, November 27, 2000.
12. Robert Karniol, "Power to the People", Jane's Defence Weekly, Surrey, UK, July 12, 2000.
13. Edward Timperlake and William C. Triplett III, "Red Dragon Rising: Communist China's Military Threat to America", Regnery Publishing Inc., Washington, D.C., 1999.
14. J. S. Bajwa, "Modernisation of the PLA: Gauging its Latent Future Potential", Lancer Publishers, New Delhi, 2002, pp. 216. Cited from Michael Pillsbury, "PLA Capabilities in the 21st Century: How does China Assess its Future Security Needs?" Article in Larry M. Wortzel, ed. "The Chinese Armed Forces in the 21st Century", pp 113-114.
15. Greg Keizer, "China Develops Cyberwar First Strike Strategy: Viruses could Attack Overseas Computers", Computerworld.com, May 30, 2007 at http://www.pcadvisor.co.uk/news/index.cfm?newsid=9527
16. Saibal Dasgupta, "China Keeps Vigil on its Borders: Chinese Army uses more than 10,000 Officers with Top Degrees in Information Technology", Times of India, June 13, 2007.
17. Mac William Bishop, "China's Cyberwarriors", Foreign Policy, September/October 2006 at http://www.foreignpolicy.com/story/cms.php?story_id=3553
18. Colonel Narendra Singh, "Chinese Armed Forces", USI Journal, New Delhi, October-December 1998, pp. 587-608.