DRAGON'S INFORMATION WARFARE: IMPLICATIONS FOR INDIA

RAJ MONGIA

INTRODUCTION

In recent years, China has demonstrated an intense fascination with information warfare. The potential advances in Chinese IW doctrine and capabilities have direct implications for Indian national security. The ability of China to conduct information warfare against India in peacetime, confrontation or conflict could pose severe challenges to Indian defence apparatus.

Information warfare is comprised of operations directed against information in any form, transmitted over any media, including operations against information content, its supporting systems and software, the physical hardware device that stores the data or instructions, and also human practices and perceptions. Sun Tzu said:

> "*. . . attaining one hundred victories in one hundred battles is not the pinnacle of excellence. Subjugating the enemy's army without fighting is the true pinnacle of excellence*." Mao Tse Tung further elaborates "*To achieve victory we must as far as possible make the enemy blind and deaf by sealing his eyes and ears and drive his commanders to distraction by creating confusion in their minds.*"

Wing Commander **Raj Mongia** is is a serving IAF officer and a Research Fellow at the Centre for Air Power Studies, New Delhi.

The term Information Warfare (IW) is primarily a concept involving the use and management of information technology in pursuit of a competitive advantage over an opponent. Information warfare may involve collection of tactical information, assurance(s) that one's own information is valid, spreading of propaganda or disinformation to demoralise or manipulate the enemy and the public, undermining the quality of opposing force information and denial. It is closely linked to psychological warfare.

People's Liberation Army (The PLA) has been quite aware of continuous changes in geo-political and geo-strategic contexts, as well as the changing nature of warfare. It has fashioned its responses by evolving appropriate military doctrines and strategies to meet future threats and challenges. Thus, modern conditions' and thereafter from 'limited local war' to 'limited war under high tech China's military doctrine' has over the years undergone a transition from people's war to 'people's war under informationalised conditions'.

The concept of limited war under high tech conditions was formulated as a response to 'Operation Desert Storm' and the lessons learnt from it, especially in the areas of information technologies and knowledge-based warfare. China's November 2004 White Paper on National Defence outlines the acceleration of a Revolution in Military Affairs (RMA) with Chinese characteristics by building an 'informationalised' force. 'Limited war under high tech conditions', which remained in force for over 10 years, has now been replaced by 'local war under informationalised conditions'' after studying the lessons of the Second Gulf War, 'Operation Enduring Freedom' in Afghanistan and 'Operation Allied Force' in Kosovo. The White Paper mentioned the main objective of PLA as:

> *"The PLA, aiming at building an informationalised force and winning an information war, deepens its reforms, dedicates itself to innovation, improves its quality and actively pushes forward the RMA with Chinese characteristics with informationalisation at its core."*

Though the term 'informationalisation' has not been clearly defined, what can be inferred is that it covers a wide ambit and includes intelligence based

weaponry besides all elements of command, control, computer, communications, intelligence, surveillance and reconnaissance (C4ISR) and traditional components of information warfare. While informationalisation is only a sub-set of the RMA, with Chinese characteristics, information warfare is a sub-set of informationalisation. But at the national and strategic levels, it transcends the military aspects and becomes an important tool for shaping perceptions and belief systems of adversaries and competitors on a higher plane. The 2004 White Paper, among other things, makes certain observations and places emphasis and focus on:

The concept of limited war under high tech conditions was formulated as a response to 'Operation Desert Storm' and the lessons learnt from it, especially in the areas of information technologies and knowledge-based warfare

- Means of information operations and automated command systems, information measures, sound organisational structures and advance weaponry and equipment, which possesses an integrated and complete array of information support and operational means.
- Promotion of informationalisation of missiles and equipment, and improvements in communications and reconnaissance capabilities, especially of the. Second Artillery Force.
- A series of projects on military information systems have been completed and information technology elements have been incorporated into battle systems and development support to military information structure has been guaranteed.
- Development of new military and operational theories and increased emphasis on training for information warfare.
- Integration of military and civil resources for efficient information mobilisation mechanisms for exploiting synergies.

IMPORTANCE OF INFORMATION WARFARE

Given the above context, one can get an insight into evolution of Chinese theories and concepts on Information Warfare (IW). As with all its military theories and

Informationalisation is only a sub-set of the RMA, with Chinese characteristics, information warfare is a sub-set of informationalisation

strategic perspectives, Chinese traditional wisdom and strategic thought is applied to all new concepts and precepts originating from the US, Russia or elsewhere. The first wave of Chinese writings on IW appeared in the mid-1990s following the success of US information technologies in the first Gulf War of 1991. Though this war was a defining event for all militaries of the world, its impact on the PLA was greater because of the aspirations of the Chinese political and military leadership towards acquiring comprehensive national strength. The PLA was first off the block in developing theories of IW and adapting Western concepts to suit local conditions. A PLA General, writing on challenges and importance of IW, observed:

> *"In near future, Information warfare will control the form and future of war. We recognise this developmental trend of information warfare and see it as a driving force in China's military and combat readiness. This trend will be highly critical to achieve victory in future wars."*

The General further emphasised that China must use a practical combination of IW and Maoist and Marxist military thought to guide IW issues under military construction. The military must study ways of using inferior equipment to achieve victory over the enemy's superior equipment. He advocated study on how to conduct 'People's war in IW domain'. The underlying theme of Chinese concepts are based on IW, and on exploiting own strengths. The other fundamental assumption is that superior tactics can compensate for inferior technology. has been emphasis on devising ways and means to attack an enemy's weaknesses and vulnerabilities

PEOPLE'S WARFARE IN INFORMATION WARFARE CONTEXT

According to some Chinese military analysts, because of the increasing relevance of information technology (IT) to people's lives, individuals who take part in IW are not all soldiers and that anybody who understands

computers may become a fighter. IW is inexpensive as the targeted party can be delivered a paralysing blow through the net and it may be difficult for the latter to discern where the attack originated. Large amount of useless information can be created to block or stop the functioning of an adversary's information system. Thus, a People's War in context of IW can be carried out by hundreds of millions of people, using open-type modern information systems. Even political mobilisation for war can be achieved via the internet, by sending patriotic e-mail messages and by setting up databases for education. This finds further support from another Chinese author, who observes that:

> *"even as … government mobilized troops, the numbers and roles of traditional warriors will be sharply less than those of technical experts…since thousand of personal computers can be linked up to perform a common operation, to perform many tasks in in place of a large-scale military computer, an IW victory will very likely be determined by which country can mobilize the most computer experts and part-time fans… That will be a real People's War."*

Preparing for people's war is a recurring theme in Chinese writing, as IW will be carried out by the PLA and society as a whole. This concept has found practical expression in turning some of the 1.5 million reserve forces into mini-IW regiments. The People's Armed Forces Department (PAFD) has reportedly organised militia/ reserve IW regiments at district levels in many provinces. For instance, in Echeng district of Hubei province, the PAFD has a network warfare battalion as well as electronic warfare, intelligence and psychological warfare battalions, and also a training base for IW activities. The PAFD has also carried out 'Informaticised People's Warfare Network Simulation Exercise'. A version of this concept was also put into practice following the bombing of the Chinese embassy in Belgrade on May 8, 1999, during 'Operation Allied Force'. The Chinese hacked a number of US political, military and diplomatic web sites, and also carried out a network battle by mobilising thousands of net users for sending emails and viruses. This caused servers to crash, paralysing a large number of web sites.

CYBER WARFARE

Concerns about China's net force were heightened after the aforementioned attacks on US computer systems and after the Chinese militia carried out IW exercises, which included India, the US, Taiwan and Japan as target countries. The aim of such training was to disrupt critical infrastructure like banking, power supply and telecommunication networks in the target country as part of China's strategy of asymmetric approach to warfare. In the cyber domain, the Chinese have adopted three methods for targeting such networks; the first is the use of e-mails for planting viruses; then phishing and lastly, the introduction of 'intelligent trojans' and 'vacuum trojans'. Diverse routes of planting trojans and viruses have been used to attack critical PCs, which in turn send out files or cause malfunction. Hackers' tools are becoming more robotic and simple; for instance, a vacuum trojan will extract information from a pen drive automatically when connected to a USB port. It is also believed that the next step could be planting the targeted sites with the more difficult to detect fake data or partially fake data.

In Nanjing, the PLA has developed more than 250 trojans and similar tools. Here, it needs to be remembered that foreign companies like Network Solutions, were made to hand over 300 computer viruses by the Ministry of Public Security's lab in an effort to speed up the certification of antivirus products . Further, the Chinese Academy of Sciences, which provides suggestions about national information security policy and law, has established the State Lab for Information Security. The lab has 'National Attack Project' as one of its research programmes. Also, select professionals have been inducted into militia organisations to boost combat capabilities in future wars. Thus, China has been paying much attention to offensive strategies in cyberspace even as it concentrates on defensive IW.

DEFINITION AND GOALS OF INFORMATION WARFARE

The Chinese understanding of IW, which was initially based on western concepts, has increasingly moved towards evolving its own orientation. Chinese experts believe that IW's essence is the sum of information capabilities capable of breaking the will to resist by attacking an enemy's

cognitive understanding and convictions, forcing it to give up all resistance and terminate the war. The goal is to "force enemy to regard their goal as our goal, to force the opponent to give up the will to resist and end confrontation and stop fight by attacking enemy's perceptions and belief via information energy." Xie Guang, the then Vice Minister of Science and Technology and Industry for National Defence, defined IW in December 1999 thus: "IW in military sense means overall use of various types (of) information technologies, equipment and systems, particularly his command systems, to shake determination of enemy's policy makers and at the same time, the use of all the means possible to ensure that that one's own systems are not damaged or disturbed." This definition apparently includes the aspects of IW's goals at the larger national level. A further elaboration was done by two senior PLA colonels, who described IW as consisting of five major elements and two general areas. The five elements are:

The goal is to "force enemy to regard their goal as our goal, to force the opponent to give up the will to resist and end confrontation and stop fight by attacking enemy's perceptions and belief via information energy"

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

The two general areas are information protection (defence) and information attack (offence). Information defence means preventing the destruction of one's own information systems, ensuring that these systems

can perform their normal functions. In future wars, key information and information systems will become "combat priorities", the key targets of enemy attack. It also includes many other manifestations of IW like computer virus warfare, precision warfare and stealth warfare, all dependent in some manner on information and software programmes.

INFORMATION OPERATIONS

Information Operations (IO) are specific operations and are considered to be at the core of IW, in the same manner as IW is considered to be at the core of informationalisation. In fact, IO is a manifestation of IW on the battlefield. It can be both of the defensive and offensive types, and can be conducted at the strategic, operational, campaign and tactical levels at times of peace, wars and crises. Principles of IO have been defined by Chinese military authors to include centralised command, decentralised control (multi-level power delegation), multi-dimension inspection and testing, timely decision-making and integration of military and civil actions with focus on key links. Major General Dai Qingmin, Director of PLA's General Staff responsible for IW and IO (and also ex-Commander of PLA's IW Centre in Wuhan) observes that integrated and joint information operations give more scope and purpose to people's war. (In fact, jointness and integration is a major theme of the 2004 White Paper). He defines IO as a series of operations with an informationalised environment as the basic battlefield condition, with military information and information systems as the direct operational targets and electronic warfare (EW) and computer networks as the principal form. He has outlined various IO strategies because, as mentioned earlier, according to the traditional Chinese approach strategies can compensate for inferior equipment and technologies and, in the case of IO, it may also compensate for gaps in information or poor information about the enemy. Some of the IO strategies are:

- Jamming or sabotaging an enemy's information or information system.
- Sabotaging an enemy's overall information operational structure.
- Weakening an enemy's information fighting capacity.

- Dispersing enemy forces, arms and fires while concentrating own forces, arms and fire.
- Confusing or diverting an enemy and creating an excellent combat opportunity for on self.
- Diverting an enemy's reconnaissance attempt and making sufficient preparations for it.
- Giving the enemy a false impression and launching surprise information attack on him at the same time.
- Blinding or deafening an enemy with false impressions.
- Confusing an enemy or disrupting his thinking.
- Making an enemy believe that what is true is false and what is false is true.
- Causing an enemy to make a wrong judgement or take wrong action.

In the IW exercises conducted by PAFD, 10 methods of IO were specified and these can be viewed as tactics in the electronic battlefield. These are:

- Planting information mines
- Conducting information reconnaissance
- Changing network data
- Releasing information bombs
- Dumping information garbage
- Disseminating propaganda
- Applying information deception
- Releasing clone information
- Organising information defence
- Establishing network spy stations

COMPUTER NETWORK OPERATIONS

In Chinese writings on Information Warfare, networking has also been the focus of discussions. The recent emphasis on jointness and integration apply equally to integrating various military networks. A critique by Timothy Thomas notes that the Chinese feel it necessary to prepare for a "network people's war". Computer network warfare has been included by Dai Qing

INEW lays stress on coordinating and integrating all aspects of C4ISR and weapon platforms and weapon systems to produce the desired effects at the target end

as one of the six forms of IW (i.e. operational security, military deception, psychological warfare, electronic warfare, computer network warfare and physical destruction). Though there is no evidence of a formal Chinese doctrine, Chinese theorists have coined the term "Integrated Network Electronic Warfare" (INEW) and this has also been referred to by Timothy Thomas as a half cousin, given its similarities and points of divergences to the US approach.

INEW has been described as a series of combat operations that integrate electronic warfare and computer network warfare measures to disrupt the normal operation of an enemy's battlefield systems while protecting one's own with the objective of attaining information superiority. The essence of computer network warfare (CNW) is "to disrupt layers in which information is processed, by seizing and maintaining control of network space". EW is targeted at networked information systems and informationalised weapon systems in order to increase combat effectiveness. According to Dai, INEW is necessary for system to system confrontation on the informationalised battlefield, as systems are centres of gravity. Any disruption in system will lead to disconnect between the people and weapons. Thus, INEW lays stress on coordinating and integrating all aspects of C4ISR and weapon platforms and weapon systems to produce the desired effects at the target end. The effectiveness of weapon platforms and network systems is directly proportional to its levels of integration. As in other spheres, integration produces a combat capability greater than the sum of its parts and, this is true for information operations as well.

China's computer network operations (CNO) comprise network attacks, defence, and exploitation. According to the Pentagon's Annual Report for 2005 to the Congress on China's military power, the PLA views CNO as critical to seize the initiative and "electromagnetic dominance" early in a conflict, and as a force multiplier. This concept outlines the integrated use of electronic warfare, CNO and limited physical strikes against key C4ISR

nodes to disrupt an enemy's battlefield network information systems. It is believed that the PLA has established information warfare units to develop viruses to attack enemy computer systems and networks, and tactics to protect friendly computer systems and networks. The PLA has increased the role of CNO in its military exercises. Although initial training efforts focused on increasing the PLA's proficiency in defensive measures, recent exercises have incorporated offensive operations, primarily as first strikes against enemy networks.

Computer network attack is the most effective means for a weak adversary to fight a strong one

The main area of weakness that the Chinese espy, especially with regard to US forces, is the deployment phase. US forces are largely dependent upon computer and communication systems, both military and nonmilitary, and the particularly weak links in the logistics network systems make them susceptible to computer network attacks. Logistics network systems may be relatively easy to penetrate compared to other C4 systems though it will be more useful to penetrate command and information links. However, the priority of Chinese CNW seems to be to prevent the force from deploying at the first place and thereafter breaking the linkages between decision-makers and weapon platforms. This approach rhymes with the oft-stated Chinese strategy of attacking weaknesses and avoiding strengths of the enemy. As observed by James Mulvenon, Chinese strategists theorise that:

- Computer network attack is the most effective means for a weak adversary to fight a strong one.
- It can be used as a means to deter the enemy.
- It has longer range than the conventional power projection assets, as long distance surveillance and precise powerful and long distance attacks are available to the military.

PSYCHOLOGICAL OPERATIONS AND INFORMATION WARFARE

Another important component of information Warfare with Chinese characteristics is psychological warfare. Chinese doctrine has traditionally

focused more attention on the psychological dimensions of IW, including deception, though of late they have also been paying equal, if not more, attention to the technological dimensions. The target in psychological operations is always the people and decision-makers, so that their will and perceptions are attacked to alter their beliefs, goals and behaviour. This is aimed at both military and civil components of an adversary's populace. Psychological operations comprise of manipulation of media to support military efforts and include conventional methods of propaganda like distribution of leaflets, radio and TV broadcasts, and other means of communication. Like most of the components of IW, psychological operations are a continuum of actions in peacetime, crisis time and war time.

In August 2005, the PLA conducted a joint exercise, involving not only all its services but also troops from Russia. The exercise involved distribution of leaflets over the opponent, electronic warfare to confuse incoming missiles and adoption of electronic counter measures. These exercises involved the use of live missiles and ammunition, and showcased precision warfare capabilities as well as the latest military equipment. These exercises could also be said to have had a psychological dimension for deterring Taiwan or those aiding it in its political objectives. Here, it can be argued that the Chinese appear to have taken a leaf out of the US forces' tom-tomming of the awesome power of their arsenal and military capabilities before the start of 'Operation Iraqi Freedom', which had the effect of lowering the morale of the Iraqi military. The US forces also air dropped over 31 million leaflets for propaganda purposes besides physically attacking Iraqi forces' command and control networks based on fibre optic lines and radio and computer servers. US forces had been issued cyber-guidance as early as February 2003 for operations in Iraq. The PLA has thus been quick to absorb lessons on IW from 'Operation Iraqi Freedom'.

The Chinese also observed the power of media when CNN's broadcast of a US soldier's body being dragged through the streets of Mogadishu transformed perceptions of victory into defeat. Authors of the Chinese book titled Unrestricted Warfare reflected on the incident thus: Did CNN's

broadcast of an exposed corpse of a US soldier in the streets of Mogadishu shake the determination of the Americans to act as the world's policeman, thereby altering the world's strategic situation? And should an assessment of wartime actions look at the means or the results?

PLA'S IW/EW CAPABILITIES

The 2004 White Paper shows that the Chinese military has understood that there is a large and expanding technology gap between it and modern militaries, especially that of the US. China's leaders, including President Hu Jintao, have ordered the PLA to pursue "leap ahead" technologies and "informationalised" capabilities to increase weapons' mobility, firepower and precision. This perspective applies to IW also.

The Central Military Commission's (CMC) Third or Technical Department of General Service Headquarters is responsible for strategic SIGINT and has established a number of monitoring stations to intercept signals from countries like India, Taiwan, Japan, South Korea and others. The PRC also established a Fourth Armed Forces Department in 1990 to look after offensive and defensive IW activities. It has also built "an information warfare simulation centre" for training its corps of network warriors. The centre uses high technology simulation skills and equipment to simulate information warfare and its environment. The Fourth Department has special detachments and units that manage and direct SIGINT and EW operations for the PLA at all levels and includes operations of the Air Force and the Navy.

The PRC has completed one million km of fibre optics line and communication infrastructure called "Eight Horizontal Grids and Eight Vertical Grids" supported by satellite, ground mobile receiving stations and ground to air data links. With technologies obtained from Western countries and by exploiting its booming commercial IT and telecommunications sector, it has improved the quality of its military programmes. The PLA has acquired and deployed a wide variety of air, sea and land-based intelligence, surveillance and reconnaissance (ISR) systems to enhance its ability to detect monitor and target military activities in Asia and West

Both military and civil sectors are actively exploring IW concepts which could lead to developing a corps of network warriors to defend

Pacific Ocean. Some of the latest programmes include electro-optics, synthetic aperture radar, over the horizon radars, and surveillance systems that can detect stealth aircraft.

EW is a key element in the PLA's 'Three Attacks and Three Defences' strategy (attack stealth aircraft, cruise missiles and helicopters; defend against precision strikes, electronic warfare, and enemy reconnaissance) to meet the requirements of 'local war under high tech conditions' which has now progressed to 'local war under informationalised conditions'. Both military and civil sectors are actively exploring IW concepts which could lead to developing a corps of network warriors to defend China's telecommunication, command and information networks while uncovering vulnerabilities of adversaries' networks.

At the national level, China has a C3I system based on fibre optic cables, satellite communications, micro-wave links, tropo-scatter communications and automated command and control systems. The PLA has both secured and non-secured telecommunications and has an army wide data communication network and integrated field operations communication system. Its WAN is capable of supporting peacetime operations within Chinese borders and limited pre-planned operations along China's periphery but is inadequate for large-scale joint operations.

The Chinese Army has a family of battlefield ELINT systems like DZ 9002 that detect, intercept, analyse and record an adversary's signal emissions. DZ 9001 has been developed both for defensive and offensive electronic counter measures (ECM). DZ 9300 is a man-packed radar reconnaissance system meant for special operations forces and rapid reaction forces. A bodyguard laser countermeasures system has also been developed to counter precision-guided munitions guided by laser emissions. There are also a variety of jamming systems with the ground forces.

The PLA Air Force is developing capabilities in airborne warning and control systems (AWACS), airborne early warning, and ECM aircraft and

UAVs. Shaanxi Y-8 has been designed for special EW, ELINT and ECM missions. This aircraft was first observed in operation in the summer of 2004 and it is believed that some of its equipment may be from the US Navy's EP-3 ELINT aircraft that made an emergency landing in Hainan in April 2001. Another version of the Y-8 aircraft is 'Balance Beam' airborne early warning aircraft meant for tactical ISR, EW and ELINT missions. It made its maiden flight in 2001 and its finalised version Y-8 F600 flew in January 2005. The PLA Air Force is planning for 4-6 AWACS and has about 20 other dedicated ELINT aircraft like HD-5, TU-154M and HZ-6. HD-5, an older version, is being replaced by HZ-6 which has improved capabilities. UAV's configured for ELINT and EW missions are also in use. In July 2002, the PLA inducted the Israeli anti-radar hunter killer HARPY UAV.

The Chinese Navy also has over a dozen ships and several trawlers for various electronic warfare missions. Four Yuan Wang and Shiyan class ships monitor space events and are capable of collecting and monitoring missile and satellite telemetry data and communications. Chinese industry has developed three types of systems, based on Soviet-era systems, which have been further upgraded and modernised.

Space is another area where the Chinese have been making rapid advances, especially in the field of ISR and anti-satellite technologies. China considers space as a 'commanding height' and it plans to control space and win the information war after having built up an informationalised PLA. In 2003, the PLA had six dual-use dedicated satellites for military purposes. In 2004, China placed 10 satellites into orbit and has a similar schedule through 2006. It hopes to have more than 100 satellites in orbit by 2010, and launch an additional 100 satellites by 2020. In the next decade, Beijing will most likely field radar, ocean surveillance, and improved film-based photo-reconnaissance satellites. China will eventually deploy advanced imagery, reconnaissance, and Earth resource systems with military applications. China's ZY-2 payloads have digital imagery reconnaissance capabilities and have worldwide coverage. Beijing also tested new film-based imagery satellites and small digital imagery satellites in 2003 and 2004. It is also developing its own GPS navigation system based on the Beidou series of

Attaining information superiority has become one of the most important objectives to be achieved in the era of knowledge age warfare

navigational satellites. The PLA possesses anti-GPS jammers obtained from Russia, which however may not be very effective against the NAVSAT satellite system of the US.

China is also developing electronic intelligence (ELINT) and signals intelligence (SIGINT) reconnaissance satellites. These digital data systems will be able to transmit directly to ground sites, and China may be developing a system of data relay satellites to support global coverage. Furthermore, Beijing has acquired mobile data reception equipment that can support more rapid data transmission to deployed military forces and units. China is developing micro satellites for remote sensing as well as for putting into place networks of electro-optical and radar satellites. In April 2004, Beijing launched a micro satellite with a probable imagery mission. China is also conducting research to develop ground-based laser ASAT Weapons. All these capabilities will contribute to China's prowess in the field of information warfare.

IMPLICATIONS FOR INDIA

Attaining information superiority has become one of the most important objectives to be achieved in the era of knowledge age warfare. The concept of information superiority is somewhat analogous to similar concepts of air, sea or space superiority. This is because proper use of information is as lethal as other kinds of power. Further, the concept of information superiority leads us to attainment of decision superiority. Information operations are increasingly being considered as important as sea, land and air operations. Information operations can vary from physical destruction to psychological operations to computer network defence. Well conducted joint information operations with new RMA technologies, improved organisations and doctrine will greatly contribute to a successful and decisive outcome.

It is in this context that a Defence Information Warfare Agency (DIWA) under the Integrated Defence Staff Headquarters has been formed to

coordinate efforts of the three services and certain other agencies to handle all aspects of information warfare. The Indian concepts of IW are generally based on Western concepts and according to the 2004 Army Doctrine, IW encompasses the elements of command and control warfare, intelligence based warfare, electronic warfare, cyber warfare, psychological warfare and network centric warfare, military deception and secrecy as well as media support. Though the three Services have different set ups for IW activity, DIWA is the nodal and apex policy-making body to formulate joint and integrated responses to IW challenges. Therefore, an IW doctrine needs to be formulated, which it is believed, is under the process of being evolved by DIWA. However, it is at operational levels that weaknesses in our IW efforts exist. There is a need for joint linkages and joint planning to synchronise our response to all elements of information warfare.

The Indian armed forces have made considerable progress in establishing C4ISR networks. But given that these are service wise, there is a need for establishing a Joint Inter-Services Network. The other areas that need attention are:

- There is a need to adopt a similar model in our Territorial Army units. Even though In the era of cyber warfare, information warfare and net wars, information systems, both civil and military networks, should have adequate redundancy, survivability and electronic security.
- For optimisation, the strengths of our IT infrastructure and industry and advancements in satellites and radio-based systems should be jointly exploited by the military and civil sectors.
- Joint network and individual services networks should be able to function in all environments including nuclear. For instance, they should be hardened against or be resistant to an EMP attack.
- We need to induct a wide variety of military satellites for upgrading our strategic ISR, SIGINT, ELINT, COMMINT, imagery and navigation capabilities.
- We need to reflect on the Chinese model of net force based on their militia and examine whether there Computer Emergency Response Teams (CERT) at national and lower levels have been formed to respond

to cyber attacks on civilian infrastructure, the concept is more defensive in nature. A pro-active concept like that of net force may be more appropriate.

CONCLUSION

China sees IW as a field where asymmetric strategies can be used to better its rivals, especially the ones with better technological capabilities. It has applied People's War concept in the context of IW to leverage the availability of a large number of civilian IT experts. Simultaneously, it has not neglected the technological aspects. Over the years, it has acquired state-of-the-art technologies from the West and Israel, and as the Cox Report of May 1999 revealed through pilferage and spying, to upgrade its arsenal.

China has a large reservoir of scientists and a booming economy, which will help it in acquiring improved capabilities in the sphere of IW. It has made rapid advances in the field of IT and space-based systems, which will assist it in closing the technological gap with its peer competitors.

IW is important at the national, strategic and operational levels. At the national level, the aim is to alter the perceptions of the adversary so that victory can be achieved without fighting or at the lowest cost. Militaries all over the world have recognised IT and IW as force multipliers and as key battle winning tools. The electro-magnetic spectrum, a key component of the information domain, has become the new high ground to be captured for success of operations, thus highlighting the operational aspects of IW. China's rising military power has created concerns not only for the US but also its neighbours, which are equally if not more concerned of the possible destabilising effects of a likely assertive China. India and other neighbours need to evolve holistic strategies to safeguard their information domains and protect them from a variety of information attacks.