CHINA'S ELECTRONIC AND CYBER WARFARE CAPABILITIES

SANJAY PODUVAL

Informationised arms . . . together with information systems, sound, light, electronics, magnetism, heat, and so on, turn into a carrier of strategies.

— Maj Gen Dai Qingmin

In the early 1990s, the People's Liberation Army (PLA) responded to the altered form of warfare by quickening the Research and Development (R&D) of advanced conventional platforms, as set by the then emerging high-tech combat environment. But, after analysing the series of anti-terror wars led by the US, the PLA has now realised that systems integration is more important than individual hi-tech hardware. Therefore, in 2002, China substantially revised its 1993 national defence strategy of fighting a regional war under hi-tech conditions to a new strategy of fighting a "regional war under the condition of informatisation." This sweeping change initiated a new phase in Chinese military modernisation programmes with the focus being hinged on integrating new military theories and concrete reforms. Central to this theme is Information Technology (IT) which is the principle driver in the present-day global military and economic change.

These extensive military modernisation programmes have fundamentally transformed the People's Republic of China's (PRC's) ability to fight high-tech

* Wing Commander **Sanjay Poduval** is a Research Fellow at the Centre for Air Power Studies, New Delhi.

The Chinese military, using increasingly networked forces capable of communicating across Service arms and among all echelons of command, is pushing beyond its traditional missions focussed on Taiwan towards a more regional posture.

wars. The Chinese military, using increasingly networked forces capable of communicating across Service arms and among all echelons of command, is pushing beyond its traditional missions focussed on Taiwan towards a more regional posture. This modernisation effort, known as informationisation/informatisation, is guided by the doctrine of fighting a "local war under informationised conditions," which refers to the PLA's ongoing effort to develop a fully networked architecture capable of coordinating military operations on land, in the air, at sea, in space and across the entire Electro-Magnetic (EM) spectrum. Adhering to this line of thinking, the PLA is working towards a unified C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance) system and IT-based networking for better cooperation and coordination within the Services and between the Services in the battlefield. The final goal of this programme is to realise an unobstructed and digitalised transfer of information between all systems: at the strategic, operational and tactical levels, among the Services and between platforms.

In Chinese writings, Electronic Warfare (EW), along with networking, has been the focus of discussions which in many ways is analogous to the American concept of Network-Centric Warfare (NCW). The emphasis on jointness and integration applies equally to integrating various military networks. Chinese theorists have coined the term "Integrated Network Electronic Warfare" (INEW) which indicates that they aim to amalgamate NCW operations with EW. This implies that the Chinese view EW from a systems approach and not as a separate or distinct element of war-fighting. Informatisation is, thus, singled out as the driving force for PLA transformation. This reflects a new understanding about the type of war the PLA expects to face in the future: even if the combat is between conventional platforms, the key to victory are the IT systems. As a consequence of their

emphasis on IT and networking, the Chinese have realised the importance of cyber warfare. The underlying theme of cyber warfare ties in perfectly with their concept of the assassin's mace, *Sha Shou Jian* (literally "killing hand club"). Given the above context, the aim of this paper is to provide an insight into the Chinese capabilities and concepts of INEW and cyber warfare.

The PRC has completed one million km of fibre optics line and communication infrastructure called "Eight Horizontal Grids and Eight Vertical Grids."

PLA'S INEW CAPABILITIES

China's 2004 White Paper shows that the Chinese military has understood that there is a large and expanding technology gap between itself 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 "informationised" capabilities to increase weapons' mobility, firepower and precision.

In response to this, the Central Military Commission's (CMC's), Technical Department of General Service Headquarters responsible for strategic Signals Intelligence (SIGINT) has established a number of monitoring stations to intercept signals from countries like India, Taiwan, Japan, South Korea and others. The PRC's Fourth Armed Forces Department which looks after offensive and defensive Information Warfare (IW) activities has set up "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 navy.[1]

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

1. Manuel Cerejo, "China, Cuba and Information Warfare, Signal Intelligence, Electronic Warfare and Cyber Warfare," at http://www.futurodecuba.org/ChinaandInformationWarfare4.htm

and ground-to-air data links.[2] At the national level, the C3I system is 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 peace-time operations within Chinese borders and limited pre-planned operations along China's periphery, with limited capability for large-scale joint operations.

With technologies obtained from the 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 the West 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 informationised 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 the vulnerabilities of adversaries' networks.

RESEARCH AND DEVELOPMENT

The Chinese R&D clearly recognises the important role that electronic warfare plays in the informationisation of their PLA. Experiments and trials are carried out with an emphasis on appreciating the effect on operating systems and frequencies. In the Chengdu Military Region (MR) experiments are continuously carried out to test and evaluate the jamming effectiveness

2. Abe C. Lin, "Comparison of Information Warfare Capabilities of the ROC and PRC," at http://cryptome.org/cn2-infowar.htm

from the opposing side. They articulate that the traditional jamming parameters of measuring signal-to-noise interference ratio at the receiver, maximum transmission range at the transmitter site, detection zone (specifically for radar systems), the suppression coefficient, the discover probability, and the deceit probability are only effective in a field test situation and are essentially worthless in a war as the jamming side cannot possibly obtain these evaluation data on the enemy directly. This indicates that their insight and analysis most closely resembles what one should expect to encounter when facing an informationised PLA. It is also suggests the steps they will take to ensure training in a real war scenario.

In modern aerial warfare, possessing hundreds of fighters and bombers counts for little if they cannot be effectively and efficiently deployed against an adversary.

On the "Multi-Signal Jamming Technology in [a] Complex Environment", Li Dongxin, a researcher from the National Keu Lab of Information Integrated Control in the Chengdu MR says that the two main radar jamming technologies used for PLA Electronic Counter-Measures (ECM)—multi-pulse velocity-range decoys and multi-pulsed false target jamming—are intended to target a pulsed-Doppler radar system but are not very effective against phased array radars. Specifically, Dongxin's conclusion is that in an increasingly complex multi-signal environment, ECM equipment has no choice but to make fundamental improvements.[3]

Chinese AEW, ELINT and JSTAR Developments

The Chinese military appreciate very well that in modern aerial warfare, possessing hundreds of fighters and bombers counts for little if they cannot be effectively and efficiently deployed against an adversary. They are, therefore, in the quest for the development and deployment of the Airborne Warning Control System (AWACS), Electronic Intelligence (ELINT) and Joint Strategic Target Attack Radar System (JSTARS).

3. Jorge Muniz, "Declawing the Dragon: Why the US Must Counter Chinese Cyber-Warriors," http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA502899&Location=U2&doc=GetTRDoc.pdf

The Chinese unveiled the KJ-2000 AWACS during their 60th anniversary celebrations. This AWACS which is now in service is equipped with a domestic AESA (Active Electronically Scanned Array)[4] similar to Sweden's Ericsson Erieye radar. The radar was designed by the Research Institute of Electronic Technology (also more commonly known as the 14th Institute) at Nanjing. The Chinese officials claim that the domestic radar is capable of tracking more targets at greater ranges than the Israeli Phalcon radar which was offered to them in the late 1990s.

The Chinese have also developed the Shaanxi Y-8 into an ELINT platform. This aircraft was first sighted in the summer of 2004 near Shanghai and features a long canoe-shaped fairing under the port side of the forward fuselage, together with various blade aerials and antennas mounted on the sealed rear loading ramp. A slightly different maritime ELINT version of the Shaanxi Y-8, possibly the Shaanxi Y-8 (DZ), is undergoing flight trials for the PLA Naval Air Force[5].

The Shaanxi Y-8 platform has also been used as the basis for what is believed to be an experimental JSTARS type configuration. This aircraft features large bulged cheek fairings on either side of the forward fuselage which are believed to house a sideways looking radar. The fuselage also has various other fairings and one on the tip of the fin, which possibly houses ELINT receivers. It is not certain how many of these aircraft are flying and their capability is also not known.

The rapid advances made recently by China in the area of airborne early warning will sooner or later lead to the production and operational deployment of at least one and possibly two airborne early warning aircraft. However, the operational effectiveness of these aircraft remains to be seen. Nevertheless there is little doubt that, with billions now flowing into the Chinese economy every year, the Chinese will continue to seek to acquire advanced technology and the current evidence suggests that sooner or later, one way or another, they will start building and developing these aircraft themselves.

4. Sinodefence.com, "KongJing-2000 Airborne Warning & Control System," http://www.sinodefence.com/airforce/specialaircraft/kj2000.asp
5. http://www.spyflight.co.uk/china%20awacs.htm

China's Anti-Radiation Missile: FT-2000

The Chinese, in their quest to develop counter-measures against AWACS, and stand-off jammers have developed various versions of a surface-to-air Anti-Radiation Missile (ARM), the FT-2000 series. Developed and manufactured by the China National Precision Machinery Import and Export Corporation (CPMIEC) during the late 1990s, the FT-2000 is also believed to be capable of destroying tactical ballistic missiles, similar to the US Patriot and the Russian S-300P systems on which it is based. At present, two versions exist, the mobile FT-2000 and the fixed-based FT-2000A.

The FT-2000 is also believed to be capable of destroying tactical ballistic missiles, similar to the US Patriot and the Russian S-300P systems on which it is based.

The FT-2000 was designed to neutralise and counter airborne jamming devices. It contains a passive radar target seeker programmed to detect the specific EM signals emanating from its target and home on to them. The system is equipped with modified HQ-9 interceptor missiles, each of which is 6.8 metres long, 0.47 metres in diameter, and has a launch weight of 1,300 kg. The HQ-9 missiles give the FT-2000 a range of 12 to 100 km and an operating altitude of 3 to 20 km. The mobile system is transported and launched on an 8 X 8 cross-country launcher with four canisters that resemble those used by the S-300P.

In addition to the mobile FT-2000, China has developed a fixed-based variant, the FT-2000A. According to a recent Chinese sales brochure, the FT-2000A uses a highly-modified HQ-2 missile that has been equipped with passive radio frequency homing seekers. Each HQ-2 is armed with a 60 kg fragmentation warhead and has a range of 60 km and a maximum altitude of 18 km. Reports indicate that each FT-2000A battery consists of 12 missile launchers, each containing one missile, and a central control station. The central control station has one master passive sensor and three auxiliary passive sensors. The four sensors are capable of triangulating on EM signals in the 2- and 6-GHz frequency range, which covers most AWACS aircraft and other EM wave seeking targets, thus, earning it the nickname "AWACS

killer"[6]. In addition to its role as an anti-radiation missile system, the FT-2000 also has advanced capability against tactical ballistic missiles, although this point is seldom mentioned.[7]

According to Harris Khan a defence analyst from the Pakdef Military Consortium, the Pakistan Air Force (PAF) is actively looking to purchase a high-altitude missile air defence system, with the Chinese-built FT-2000 as the front-runner[8]. In October 2003, it was reported that China had closed a deal with its neighbour, Pakistan, to supply the latter with an unspecified number of FT-2000 missiles to counter India's early warning capabilities. The China-Pakistan deal followed India's arrangement with Israel and Russia to install three Israeli Phalcon AWACS on the Ilyushin Il-76.[9]

According to an article published in Malaysia in January 2003, the People's Liberation Army is eager to export the FT-2000 around the globe. It is, therefore, entirely possible that "AWACS killer" air and missile defence systems like the FT-2000 will soon proliferate throughout Asia, Europe, and the Middle East, a development that would introduce a multitude of strategic problems the world over.

Directed Energy Weapons

Since the invention of gunpowder, a weapon's effectiveness has no longer depended on the wielder's strength, but on the chemical energy of the propellant or explosive. While centuries of technological advances have improved the power of these materials, the basic operating principle ultimately remains the same. Modern battlefield weapons are descendents of muskets and cannons but with greater range, accuracy and

6. "FT-2000, Missile Defence Systems," http://www.missilethreat.com/missiledefensesystems/id.20/system_detail.asp
7. Richard D. Fisher, Jr., "The Impact of Foreign Weapons and Technology on the Modernisation of China's People's Liberation Army", A Report for the U.S.-China Economic and Security Review Commission January 2004, http://www.globalsecurity.org/military/library/report/2004/04fisher/part3.htm#impactonplamissile
8. Wendell Minnick, "Pakistan Targets Air Combat", http://www.defensenews.com/story.php?i=3637167, Published: July 14, 2008.
9. Bulbul Singh, "Pakistan Seeks FT 2000 Missiles to Counter Indian Warning System," *Aerospace Daily*, October 28, 2003.

power packed in them. Another revolution in weaponry is currently underway, with Directed Energy Weapons (DEWs) on the cusp of entering the domain of chemical-powered weapons on the battlefield. DEWs use the electromagnetic spectrum (light and radio energy) to attack and destroy targets at the speed of light. After decades of research and development, DEWs are becoming an operational reality. Such weapons generate streams of electro-magnetic energy that can be precisely aimed over long distances to disable or destroy targets.

Some estimates suggest that approximately 10,000 personnel, including 3,000 engineers from 300 organisations are involved in China's laser programmes alone, with perhaps 40 per cent of related R&D being conducted for defence applications.

DEWs include High Power Microwaves (HPM), high energy laser and particle beam technologies. Research is currently on in the field of high energy lasers and high power microwaves and a lot of progress has been made towards the weaponisation of the EM waves. This is one of the reasons for the change in nomenclature of ECM (Electronic Counter-Measure) to EA (Electronic Attack). A number of programmes are being actively pursued by China, Israel, Russia and the US, to name a few. Though the US is in the forefront of these technologies, countries like China and Russia have not lost sight of these weapons and are investing a lot in this field. China is currently devoting a considerable amount of resources on the tactical and strategic use of directed energy weapons for applications in areas such as air defence, anti-personnel, communications, weapons guidance and fire control, sensors, space tracking, Anti-Satellite (ASAT) and Ballistic Missile Defence (BMD). While still probably trailing behind the expertise of the US, China's DEW related R&D and applications programmes are massive and sophisticated by any international standards. China is believed to be a world leader in various specific areas. Some estimates suggest that approximately 10,000 personnel, including 3,000 engineers from 300 organisations are involved in China's laser programmes alone,

Militaries all over the world increasingly depend on space systems for various force enhancements and application functions.

with perhaps 40 per cent of related R&D being conducted for defence applications.[10]

The National Engineering Research Centre for Solid State Lasers (SSL) in Beijing is conducting R&D on solid state lasers. The SSL Shenguang-2[11] reportedly has a power output of a terrawatt. The establishment has also developed a tuneable titanium-sapphire ruby laser with a power output of 650 megawatts. They are also in the process of developing high-energy lasers to be used as ground-based ASAT weapons (China currently has the capability to damage, under specific conditions, optical sensors of satellites).

R&D is also on in China for the development of an HPM warhead, which is likely to be operational by 2015.[12] Extensive studies are also being carried out to study the effect on electronics due to HPM with the aim of developing impregnable shields not only to protect the systems delivering these weapons but also their ground-based systems if subjected to such attacks.

The DEW programmes of China have been aided by the erstwhile Soviet Union's scientific community that has been absorbed by China. Recent reports attributed to the US Defence Intelligence Agency also indicate that Israeli Aircraft Industries may have transferred key high-energy laser technologies to China. With its ASAT test in 2007 and the blinding of a US satellite in 2006, China has conveyed a message to the world that in any future conflict with it, no country will be able to use its satellites (at least, the low earth satellites) for military purposes.

INEW in Space

Militaries all over the world increasingly depend on space systems for

10. Source Jane's Defence, at http://www.aeronautics.ru/archive/research_literature/aviation_articles/Janes/topics/plasma_stealth/Directed%20Energy%20Weapons%20and%20Sensors.pdf
11. "Directed Energy Weapons and Sensors," http://www.asiafinest.com/forum/index.php?showtopic=188488, Jan 17 2009.
12 Source Jane's Defence, at http://www.aeronautics.ru/archive/research_literature/aviation_articles/Janes/topics/plasma_stealth/Directed%20Energy%20Weapons%20and%20Sensors.pdf

various force enhancements and application functions. Space force plays an increasingly critical role in enhancing information superiority, situational awareness and targeting to military forces. Space power is, therefore, a vital element which provides the ability to be persuasive in peace, decisive in conflict and preeminent in any form of combat. Having realised this, Chinese military strategists and aerospace scientists have been quietly designing a blueprint for achieving space dominance for more than a decade. Chinese military scientists have contended that support from space for warfare will become the core of future non-contact combat. The integrated space-based electronic network of combat platforms, weaponry, and C4ISR components will guide the various combat elements of the three armed Services to launch long-distance precision attacks on ground, sea, air and space targets.

Just as land dominance, sea control and air superiority have become critical elements, space superiority is emerging as an essential element of battlefield success and future warfare.

Just as land dominance, sea control and air superiority have become critical elements, space superiority is emerging as an essential element of battlefield success and future warfare. As space systems become lucrative targets, there will be a critical need to develop robust capability to ensure space superiority – as it has been for the land, sea and air dimensions. Accordingly, the PLA revamped its R&D testing and evaluation programme of the late 1990s and decided to cancel weapons projects that had been active for 10 years or longer and to direct these funds to developing so-called ''new-concept weapons'': laser, beam, electro-magnetic, microwave weapons. China also aims to develop a new generation of solid-fuel rockets to carry micro-satellites in an endeavour to establish a space network for precise positioning, communications, electro-magnetic jamming, and reconnaissance. This is perfectly in sync with their concept of INEW.

Since the space theatre of war is in outer space and more than 120 km above the earth's surface, there are no restrictions concerning national boundaries and sovereign air space. The side possessing space dominance,

can, therefore, exercise complete freedom of action. The unique, high-altitude advantages of space have strategic and decisive significance for the side exercising space dominance. It will be possible:

- To execute such offensive operations as satellite attack, missile intercept, and ground firepower support.
- To guarantee the operational independence of friendly military space forces, and to translate these advantages into information, air and sea dominance.

Without space dominance, the Chinese believe that one is actually putting oneself in the disadvantageous position of "being defeated first and then going to war."

Owing to its strategic significance, space EW—aimed at jamming, sabotaging, and destroying satellites—has become the most important way to gain information dominance in future wars.[13] As the pivotal role of space-based reconnaissance becomes increasingly manifest, various countries are rushing to develop counter-measures. Active jamming is said to be the most effective technique among asymmetrical counter-measures. It is divided into active suppressive and active deception jamming. Active suppressive jamming includes barrage, spot, and random pulse jamming. Active deception jamming includes repeater, responsive, and scattered wave jamming.

EW satellites travelling in geo-stationary orbits or 300-1,000 km orbits can conduct electronic reconnaissance and jamming in wide areas. Based on the capabilities of reconnaissance satellites, Chinese aerospace scientists have compiled the following list of "space-information counter-measures":

- Aim for the satellite's effective payload by applying suppression interference to cause overload in the satellite's receiving system, data processing system, and memory.
- Target the satellite's remote control system by:
  - Establishing a space target monitoring system to acquire the satellite's technical parameters and character information.

13. Mary C. FitzGerald, "China's Military Modernization and its Impact on the United States and the Asia-Pacific," http://www.uscc.gov/pressreleases/2007/07_03_22pr.pdf

  - Effectively detecting and analysing the satellite's operational system and down-link remote signal.
- Attack the satellite's space-to-ground communication and command nodes to weaken the connection, link, mutual operation, and networking flexibility in order to degrade its operational effectiveness.
- Use high-energy and kinetic weapons to blind or destroy the reconnaissance satellites.

Another system which is a potential target for disruption is the US Global Positioning System (GPS) network. While Chinese military experts applaud the "brilliant" performance of the US GPS in recent high-tech military operations, they continue to clarify its inevitable "Achilles' Heel." They have delineated three major weaknesses. These are especially relevant as India is well on her way to develop and deploy the GAGAN[14] and IRNSS[15] position, navigation and timing system.

- First, defeat GPS at its source by exploiting the weakness of the low orbits of navigation satellites. This could be accomplished by attacking them with ASATs or high energy laser weapons.
- Second, defeat GPS in the middle by exploiting the scattered and exposed ground stations.
- Finally, defeat GPS at the end by exploiting the fact that navigation signals are highly attenuated. After attenuation by natural causes, the ground signal is very weak and easy to jam.

Besides these, China is also developing ELINT and SIGINT reconnaissance satellites. These digital data systems will be able to transmit directly to ground sites via a system of data relay satellites to support global coverage. Furthermore, Beijing has acquired mobile data reception equipment that can support rapid data transmission to deployed military forces and units.

14. GAGAN – GPS and geo-augmented system; the Indian Space Research Organisation and Airports Authority of India are implementing a Space-Based Augmentation System (SBAS) over the Indian air space for civil aviation, called GPS and Geo-Augmented Navigation (GAGAN) to provide a seamless navigation service for all the phases of flight over Indian air space.
15. IRNSS – Indian Regional Navigation Satellite System.

Unlike India's wherein there is a clear non-military slant, the Chinese space programme has a strong military bias which permeates even the scientific, domestic, and commercial elements of the space effort.

China is developing micro-satellites for remote sensing as well as for putting into place networks of electro-optical and radar satellites. The Chinese are expanding their Computer Network Operation (CNO) initiatives to include activities that threaten the space control and supporting computer networks of their adversaries, thus, posing a significant risk to their critical war-fighting systems.

The sphere of action in space is not limited to these operations but also has tremendous potential applications in:

- Detection, tracking and destruction of ballistic missiles.
- Disrupting communication links between satellites and ground stations by 'drowning out' the signal with a more powerful 'fake' signal or by targeting ground stations via physical attacks or computer hacking.
- Misdirecting or hijacking Unmanned Aerial Vehicles (UAVs) especially those linked via satellites.
- Taking over enemy computers.

Unlike India's wherein there is a clear non-military slant, the Chinese space programme has a strong military bias which permeates even the scientific, domestic, and commercial elements of the space effort. China has a comprehensive, integrated and focussed space programme. Owing to its strategic significance, Chinese aerospace experts state that disrupting, sabotaging and destroying satellites has become the most important way to gain information dominance in future wars.

The increasing exploitation of space by China under all weather conditions will improve intelligence gathering and targeting capability across the vast expanse of the Indian landscape. There is a risk that space-based communications of our nuclear arsenal could be neutralised by Chinese ASAT capabilities. This would have an adverse effect on our nuclear deterrent if redundancy is not adequately maintained. By virtue of

having good battlefield awareness and transparency, China will be able to prioritise target selection and enhance the destructive potential of its arsenal while prosecuting air, land and sea campaigns. China's counter-space capabilities are a threat to India's limited yet valuable ISR, communication and navigation satellites, through both hard kill and soft kill options, which could deny India the much needed overall battlespace awareness. While China continues to improvise on its capabilities, indirectly it also makes Pakistan a 'proxy space power' given its penchant for proliferation of technology and capabilities. Exploitation of China's capabilities for use by Pakistan against India cannot be ruled out in any future conflict.

CYBER WARFARE CAPABILITIES

Chinese View on Cyber Warfare

Historically, the PLA based its strategic philosophy on "active defence," meaning that China would never attack someone first but would be ready to respond if attacked. The doctrine drew inspiration from Mao Zedong's theory of "protracted war," in which he argued that "we must, as far as possible, seal up the enemies' eyes and ears, and make them become blind and deaf, and we must, as far as possible, confuse the minds of their commanders and turn them into madmen, using this to achieve our own victory." The goal of this paralysing attack is to inflict a "mortal blow" [*zhiming daji*], though this does not necessarily refer to defeat.[16] However, this philosophy of active defence has changed over the past few years with the advent of the cyber age. There has been a continuous stream of open-source descriptions of both cyber units in, and offensive cyber operations by, the Chinese military. Gen Dai Qingmin in a *Military Science* article in 1999 signalled a change to the offensive posture when he opined that offence is at least as important as active defence, and "the key to gaining the initiative in operations lies in positively and actively contending with an enemy for information superiority. China should establish such a view for Information

16. James C. Mulvenon, "Chinese Information Operations Strategies in a Taiwan Contingency," http://www.uscc.gov/hearings/2005hearings/written_testimonies/05_09_15wrts/mulvenon.pdf

Chinese analysts often speak of using these attacks to deter the enemy, or to raise the costs of conflict to an unacceptable level.

Operation (IO) as 'active offence'." His view was that active offence is essential for maintaining information control, obtaining the initiative, and offsetting an opponent's superiority. Offensive information methods can help sabotage an enemy's information systems. The PLA has openly stated that US' reliance on computer systems is a huge vulnerability, ripe for exploitation. The PLA's open recognition of the need for offensive operations reflects a significant break with traditional military thought.[17]

The Chinese are developing their capabilities keeping the US in focus, for they believe that by keeping the US as the benchmark, others will easily be catered for. At the strategic level, contemporary writers view IO and CNO as useful supplements to conventional war-fighting capability, and powerful asymmetric options for "overcoming the superior with the inferior." According to one PRC author, "Computer network attack is one of the most effective means for a weak military to fight a strong one." Yet another important theme in Chinese writings on CNO is the use of computer network attacks as the spear-point of deterrence. Computer network attacks are particularly attractive to the PLA, since they have a longer range than their conventional power projection assets and a well planned computer network attack could force the enemy to surrender without fighting.

Chinese analysts often speak of using these attacks to deter the enemy, or to raise the costs of conflict to an unacceptable level. Specifically, computer network attacks on non-military targets are designed to "...shake war resoluteness, destroy war potential and win the upper hand in war," thus, undermining the political will of the population for participation in military conflict. In the modem age, cyber warfare targets computers—the core of weapons and C4I systems—in order to paralyse the enemy.

To this end, China is developing new Information Warfare (IW) measures where cyber attacks on the enemy's C4ISR will be an integral part of future

17. Lt. Col. Timothy L. Thomas, US Army (Retd.) "China's Electronic Strategies," http://www.au.af.mil/au/awc/awcgate/milreview/thomas.htm

warfare. This idea is significant because about 80 percent of US military communications facilities rely on civilian networks, creating a window of opportunity for cyber strikes.

At an operational level, the emerging Chinese IO/CW (Cyber Warfare) strategy has the following key features:

- Chinese authors emphasise Computer Network Defence (CND) as the top priority. In interviews, analysts assert their belief that the US is already carrying out extensive computer network attacks against Chinese servers. As a result, they contend that CND must be the highest priority in peace-time, and only after that problem is solved can they consider "tactical counter-offensives."
- Second, CNO is viewed as an unconventional warfare weapon to be used in the opening phase of a conflict to inflict a paralysing blow on the enemy. PLA analysts believe that a virtual incapacitating strike at the beginning is necessary, because the enemy may simply unplug the network, denying them access, thus, obviating all prior intelligence preparation of the battlefield.
- Third, IW is seen as a tool to permit China to fight and win an information campaign, precluding the need for conventional military action.
- Fourth, China's challengers, in particular the United States, are seen as "information dependent," while China is not. This latter point is an interesting misperception, given that the current Chinese C4I modernisation is paradoxically making them more vulnerable to US methods.
- Perhaps most significant, the computer network attack is characterised as a preemption weapon to be used under the rubric of the rising Chinese strategy of *xianfa zhiren,* or "gaining mastery before the enemy has struck."

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, intelligence and psychological warfare battalions, and also a training base for IW activities. 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 websites, and also carried out a network battle by mobilising thousands of net users for sending e-mails and viruses. This caused servers to crash, paralysing a large number of websites.[18]

Concerns about China's net force were taken seriously after the above mentioned 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 the 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[19] 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. The Chinese military daily, *Jiefangjun Bao* carried an article in August 2002 about the forms of network attacks. These were listed as "premeditated" (i.e. a persistent computer virus embedded in software), "contamination" (aimed at the quality of information), "strong" (referring to the forced modulation of computer viruses into electro-magnetic waves),

18. Ellen Messmer, "Kosovo Cyber-War Intensifies: Chinese Hackers Targeting US Sites, Government Says," http://edition.cnn.com/TECH/computing/9905/12/cyberwar.idg/
19. In the field of computer security, phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

and "fission" (the strong regeneration capability of a virus). All are capable of being inserted in peace-time, except perhaps the "strong" variety.

CW is inexpensive and attractive as the targeted party can be delivered a paralysing blow through the net and it will be difficult for the latter to discern the origin of the attack. A 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 the context of IW can be carried out by hundreds of millions of people, using open-type modern information systems.

The prospect of Internet-based warfare has come to the fore after a series of high-profile international attacks.

China's International Cyber Warriors

China's cyber attacks have shown a significant increase in the last decade. Some of the incursions can appropriately be construed as computer reconnaissance missions on military systems to spot vulnerabilities or plant trap doors or viruses or sleeping agents into the systems which could be activated during a crisis. This fits in well with the old Chinese saying, "A victorious army first wins and then seeks battle. A defeated army first battles and then seeks victory".

Besides the long distance reconnaissance which the electronic systems enable, the computer network attack also enjoys a high degree of "plausible deniability," rendering it a possible tool of strategic denial and deception. Cyber operations are inexpensive and easy to repudiate; the enemy country can receive a paralysing blow through the Internet, and the party at the receiving end will not be able to tell whether it is a prank or an attack from an enemy.

The cost of hi-tech strikes on government communications is falling, while the amount of damage they can inflict is growing. Among the chief threats are the cyber attacks during peace-time which aim to shut down the government machinery, financial institutions, rail, road, air traffic control systems and online communication networks or use the Internet to attack other official institutions. The prospect of Internet-based warfare has come to the fore after a series of

high-profile international attacks. In 2008, it emerged that a gang of hackers, believed to be from China, had infiltrated computer systems at the Pentagon and launched attacks on government networks in Britain, Germany, India and Australia. US officials, who have labelled the group Titan Rain, have accused them of operating under the auspices of officials in Beijing.[20]

The New York Times also reported that in a series of "sophisticated attempts" against the US nuclear weapons lab at Oak Ridge, Tennessee, Chinese hackers were able to "remove data".[21] This illustrates the alarming fact that the Chinese cyber spies are now capable of entering fortified computer networks. US Strategic Command Chief Gen James E. Cartwright told Congress in March 2007 that "America is under widespread attack in cyberspace." During Fiscal Year (FY) 2007, the Department of Homeland Security received 37,000 reports of attempted breaches on government and private systems, which included 12,986 direct assaults on federal agencies and more than 80,000 attempted attacks on Department of Defence computer network systems. As for China's part in this trend, one American cyber security analyst said that intrusions from China are showing an increasing trend and in the last three months of the last quarter of 2007, the attacks from China had almost tripled. [22]

Jonathan Evans, then chief of Great Britain's MI-5, in a confidential letter to 300 accountants, legal firms, and chief executives and security chiefs at banks, warned them that they were under "electronic espionage attack" from "Chinese state organisations." Mr. Evans noted that a number of British companies—Rolls Royce, for example—had discovered that viruses of Chinese government origin were uploading vast quantities of industrial secrets to Internet servers in China.[23]

20. Bobbie Johnson, technology correspondent, "NATO says Cyber Warfare Poses as Great a Threat as a Missile Attack," http://www.guardian.co.uk/technology/2008/mar/06/hitechcrime.uksecurity
21. John Markoff, "China Link Suspected in Lab Hacking," *The New York Times*, December 9, 2007, p. A-03, at www.nytimes.com/2007/12/09/us/nationalspecial3/09hack.html
22. Stephen Fidler, "Steep Rise in Hacking Attacks from China," *The Financial Times*, December 5, 2007, at www.ft.com/cms/s/0/c93e3ba2-a361-11dc-b229-0000779fd2ac.html. Source cites Yuval Ben-Itzhak, chief technology officer for Finjan, a Web security group based in San Jose, California.
23. Rhys Blakely, Jonathan Richards, James Rossiter, and Richard Beeston, "MI5 Alert on China's Cyberspace Spy Threat," TimesOnline, December 1, 2007, at http://business.timesonline.co.uk/tol/business/industry_sectors/technology/article2980250.ece (December 11, 2007)

In August 2007, German Chancellor Angela Merkel learned that three computer networks in her own office had been penetrated by Chinese intelligence services. A few days later, she confronted the visiting Chinese Premier directly about the attacks and demanded that China play by the rules. Premier Wen Jiabao, straight-faced, expressed utter shock and promised that his government would get to the bottom of it. He then asked for detailed information from Germany's counter-intelligence agencies to help China's security police find the culprit!!![24]

According to Richard Lawless, Deputy Under Secretary of Defence for Asia-Pacific Affairs, the Chinese are "leveraging information technology expertise available in China's booming economy to make significant strides in cyber-warfare." The Chinese military's determination to familiarise themselves and dominate to some degree the Internet capabilities is providing them with a growing and very impressive capability.

While the various governments may be reticent to reveal the vulnerabilities of their databases to Chinese penetration, the information available shows how widespread Chinese cyber attacks have become. Cyber warfare units in the Chinese PLA have already penetrated the Pentagon's unclassified but sensitive Non-classified Internet Protocol Router Network (NIPRNet) and have designed software to disable it in times of conflict or confrontation. Maj Gen William Lord, Director of Information, Services, and Integration in the Air Force's Office of War-fighting Integration admits that "China has downloaded 10 to 20 terrabytes of data from the NIPRNet already," and added, "There is a nation-state threat by the Chinese."[25]

Patriotic Hacking

At 8 am on May 4, 2001, anyone trying to access the White House website got an error message. By noon, whitehouse.gov was down entirely, the victim of a so-called distributed denial-of-service (DDoS) attack. Somewhere in the world,

24. John Blau, "German Govt PCs Hacked, China Offers to Investigate: China Offers to Help Track Down the Chinese Hackers Who Broke into German Computers," *PC World*, August 27, 2007, at www.washingtonpost.com/wp-dyn/content/article/2007/08/27/AR2007082700595.html.
25. "Pentagon Warns of Internet Incursion by Chinese Cyber-Terrorists," GCN, August 24, 2006.

hackers were pinging White House servers with thousands of page requests per second, clogging the site. Also attacked were sites for the US Navy and various other federal departments. A series of defacements left little doubt about where the attacks originated as each had a Chinese signature. The military escalated its Infocon threat level from normal to alpha, indicating risk of crippling cyber-attack. Over the next few weeks, the White House site went down twice more. By the time the offensive was over, Chinese hackers had felled 1,000 American sites.

This cyber-conflict grew out of real-world tensions. A month earlier, a US EP-3 reconnaissance aircraft flying off the southern coast of China had collided with a Chinese F-8 fighter jet. The American pilot landed safely, but the Chinese pilot was killed. China's hackers lashed out. It wasn't the first foreign attack on American sites, but it was the biggest – it was dubbed as the *First World Hacker War.* On the anniversary of this cyber war, as businesses were bracing for another round of hacking, the Chinese government is said to have successfully called for a stand-down at the last minute, suggesting that the Chinese government has a sufficient amount of control on these hackers.[26]

Patriotic hacking is increasingly carried out by sophisticated, nationalistic hacker groups and appears to have become a permanent feature of Chinese foreign and security policy crises in recent years. On the one hand, the emergence of this trend presents the PRC military and political leadership with serious command and control problems. Specifically, uncontrolled hacking by irregulars could potentially undermine the PRC's political-military coercive diplomacy strategy during a crisis. Unlike traditional military instruments such as missiles, many of the levers of computer network operations by "unofficial means" are beyond the control of the Chinese government. This could negate the intended impact of strategic pausing and other political signals during a crisis. Yet, at the same time, patriotic hacking offers several new opportunities for the PRC.

- First, it increases plausible deniability for official Chinese CNA/CNE.

26. Pamela Hess, "China Prevented Repeat Cyber Attack on US," UPI, October 29, 2002, http://www.upi.com/view.cfm?StoryID=200210291219245101r.

- Second, it has the potential to create a large, if unsophisticated set of operators who could engage in disruption activities against the adversary networks. Commentators from the intelligence community of Taiwan emphasise the use of the "unofficial power of IW" and highlight the role of non-state actors in achieving state coercion goals.

For these reasons, one could be tempted to state that the patriotic hackers are "controlled" by Beijing. Among the arguments marshalled to support this thesis is the fact that consistently harsh punishments are meted out to individuals in China for committing relatively minor computer crimes, while patriotic hackers appear to suffer no sanction for their brazen contravention of Chinese law. Other analysts begin from the premise that since the Chinese government "owns" the Internet in China, patriotic hackers must, therefore, work for the state. Still others point to the fact that a number of these groups, such as Xfocus and NSFocus, appear to be morphing into "white-hat" hackers (i.e., becoming professional information security professionals), often developing relationships with companies associated with the Ministry of Public Security or with the ministry itself. Whatever their standing in reality, because of their usefulness, these independent groups are at the least "state-tolerated" or "state-encouraged." They are tolerated not only because they are useful tools for the regime, but are, at the same time, careful not to pursue domestic hacking activities that might threaten internal stability or security and thereby activate the repression apparatus. Indeed, most of the groups have been issued constitutions or other organising documents that specifically prohibit members from attacking Chinese websites or networks. What is left to be seen is whether these state pampered groups morph into the cyber version of an E-Frankenstein monster.

Ghosts in the Net

The largest spying operation to come to light was uncovered by Shishir Nagaraja and Ross Anderson while investigating intelligence leaks at the Office of His Holiness the Dalai Lama (OHHDL) in Dharamsala. In a matter of two years, at least 1,295 computers in 103 countries, including many

belonging to embassies, foreign ministries and other government offices, as well as the Dalai Lama's Tibetan exile centres in India, Brussels, London and New York had been infiltrated. Though the fingers directly point to China, it is not clear whether there is a direct involvement of the Chinese government. The malware installed in these compromised computers besides phishing (extracting user identity and passwords) also scanned the systems for important information. The malware also has the ability to turn on the camera and audio-recording functions of an infected computer, enabling monitors to see and hear what goes on in a room. It is, however, not clear whether this facility was used. [27] GhostNet is the name given to this large-scale electronic spying operation, based mainly in the People's Republic of China. Investigators focussed initially on allegations of Chinese cyber-espionage against the Tibetan exile community, such as instances where e-mail correspondence and other data were stolen. This led to the discovery of a much wider network of compromised machines.

Compromised systems were discovered in the embassies of India, South Korea, Indonesia, Romania, Cyprus, Malta, Thailand, Taiwan, Portugal, Germany Pakistan and the office of the Prime Minister of Laos.

Despite the lack of evidence to pin-point the Chinese government in the operation of GhostNet, researchers have found actions taken by government officials from the People's Republic of China that were linked to the information obtained via the GhostNet. One such incident involved a foreign diplomat who was sent an e-mail invitation from His Holiness the Dalai Lama, but before they could follow it up with a courtesy telephone call, the diplomat's office was contacted by the Chinese government and warned not to go ahead with the meeting. Another incident was about a Tibetan woman who was interrogated by Chinese intelligence officers and was shown transcripts of her online conversations.[28]

Technical Functionality: E-mails are sent to target organisations that contain contextually relevant information. These e-mails contain malicious

27. Shishir Nagaraja and Ross Anderson, "The Snooping Dragon: Social-Malware Surveillance of the Tibetan Movement," http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-746.pdf March 2009.
28. "Tracking GhostNet: Investigating a Cyber Espionage Network," http://www.infowar-monitor.net/ghostnet; http://www.tracking-ghost.nett

attachments, that, when opened, drop a Trojan horse onto the system. This Trojan connects back to a control server, usually located in China, to receive commands. The infected computer will then execute the command specified by the control server. Occasionally, the command specified by the control server will cause the infected computer to download and install a Trojan known as Ghost Rat that allows attackers to gain complete, real-time control of computers running Microsoft Windows. Such a computer can be controlled or inspected by attackers, and even has the ability to turn on camera and audio-recording functions, if present, of infected computers, enabling monitors to perform surveillance.[29]

Shadow Network

On April 06, 2010, researchers and collaborating institutions based at the Munk School of Global Affairs at the University of Toronto published a report, *Shadows in the Clouds Investigating Cyber Espionage 2.0*,[30] which states that a Chinese network based in Sichuan province had been carrying out a spying operation for several months, targeting Indian government establishments, including security installations. According to the *New York Times,* it is possible that the operation had the blessings of the Chinese government.[31] This cyber infiltration has been named the "Shadow Network". The report documents a complex ecosystem of cyber espionage that systematically compromised government, business, academic, and other computer network systems in India, the offices of the Dalai Lama, the United Nations, and several other countries. The profile of documents recovered suggests that the attackers targeted "specific systems and profiles of users".

During the period in which the attacks were monitored, the attackers pilfered 99 documents, from India, including what appears to be one encrypted diplomatic correspondence as well as five documents marked

29. n. 27.
30. "SHADOWS IN THE CLOUD: Investigating Cyber Espionage," *2.0.* INFOWAR · MONITOR. JR03-2010. www.f-secure.com/weblog/archives/Shadows_In_The_Cloud.pdf
31. "Did China Govt 'okay' Cyber Attacks on India?," http://www.dnaindia.com/india/report_did-china-govt-okay-cyber-attacks-on-india_1368298

The above operations clearly indicate that China's cyber warfare capability is deep, pervasive and a threat not only to governments and militaries but also to foreign corporations and individuals.

"RESTRICTED" and four documents marked "CONFIDENTIAL". These documents contained reports concerning secret assessments of India's security situation in the states of Assam, Manipur, Nagaland and Tripura, as well as those concerning the Naxalites and Maoists. The documents also contained confidential information from Indian Embassies regarding international relations with, and assessments of activities in, West Africa, Russia/Commonwealth of Independent States and the Middle East, as well as visa applications, passport office circulars and diplomatic correspondence. Some of the breaches also involved Indian Embassy computers in Kabul, Moscow, Dubai, United Arab Emirates, and the High Commission of India in Abuja, Nigeria. Data was also accessed from Indian Military Engineer Services in Bengdubi, Calcutta, Bangalore, Jalandhar, the 21 Mountain Artillery Brigade in Assam, three Air Force bases and from computers at two Indian military colleges.[32]

This is a much bigger, more sophisticated, different and a more deeply focussed India specific Internet spying operation than the surveillance ring GhostNet that attacked Indian data last year. The attack made extensive use of Internet services like Twitter, Google Groups, Blogspot, blog.com, Baidu Blogs and Yahoo! Mail to automate the control of computers once they had been infected.

The above operations clearly indicate that China's cyber warfare capability is deep, pervasive and a threat not only to governments and militaries but also to foreign corporations and individuals. The Chinese government can decipher most types of encrypted e-mails and documents. China's Internet spy network is thought to be the most extensive—if not the most creative—in the world. The government's strongest tactic is a vast network of botnets—parasitic software programmes that allow their users

32. "Chinese Hackers Steal Secret Indian Documents," http://timesofindia.indiatimes.com/world/us/Chinese-hackers-steal-secret-Indian-documents/articleshow/5767793.cms

to hijack networked computers.[33] Individual bots can be building blocks for powerful conglomerations known as "botnets" or "bot armies," similar to traditional Chinese espionage. It may not be the most efficient form of cyber warfare but China wields this instrument very effectively.[34]

While much of China's Internet spying is aimed at Taiwan, it is also driven by Beijing's desire for global power status. With the United States and Russia investing in offensive and defensive cyber warfare capability, China, not wanting to be left behind, is applying its strengths and devoting its resources to stay ahead of them instead of being caught in the middle.

With its information infrastructure under tight governmental control, China can leverage its massive manpower resources in a manner that allows it to conduct far more direct and holistic cyber warfare operations than any other country. Because of the tight control over the Internet activity inside the country, virtually all information coming into and out of China can be filtered out by the flip of a switch, which is an unprecedented amount of control. Today, with current technology, the Chinese government can hack into almost anything, even without information on specific encryption programmes. It can do this not only by breaking codes but also through

33. A botnet or robot network is a group of computers running a computer application controlled and manipulated only by the owner or the software source. The botnet may refer to a legitimate network of several computers that share programme processing amongst them. Usually though, when people talk about botnets, they are talking about a group of computers infected with the malicious kind of robot software, the bots, which present a security threat to the computer owner. Once the robot software (also known as malicious software or malware) has been successfully installed in a computer, this computer becomes a zombie or a drone, unable to resist the commands of the bot commander. A botnet may be small or large depending on the complexity and sophistication of the bots used. A large botnet may be composed of ten thousand individual zombies. A small botnet, on the other hand may be composed of only a thousand drones. Usually, the owners of the zombie computers do not know that their computers and their computers' resources are being remotely controlled and exploited by an individual or a group of malware runners through Internet Relay Chat (IRC) There are various types of malicious bots that have already infected and are continuing to infect the internet. Some bots have their own spreaders - the script that lets them infect other computers (this is the why botnets are also referred to as computer viruses).
A zombie computer (often shortened as zombie) is a computer connected to the Internet that has been compromised by a hacker, a computer virus, or a Trojan horse. Generally, a compromised machine is only one of many in a botnet, and will be used to perform malicious tasks of one sort or another under remote direction. Most owners of zombie computers are unaware that their system is being used in this way.
34. "China: Pushing Ahead of the Cyberwarfare Pack," March 2, 2009, http://www.stratfor.com/memberships/132785/analysis/20090225_china_pushing_ahead_cyberwarfare_pack

less elaborate means, such as capturing information upstream on Internet servers, which, in China, are all controlled by the government and its security apparatus. If a foreign company is operating in China, it is almost a given that its entire computer system is or will be compromised. If companies or individuals are using the Internet in China, there is an extremely strong possibility that several extensive bots have already infiltrated their systems. STRATFOR sources in the Chinese hotel industry tell of extensive Internet networks in hotels that are tied directly to the Public Security Bureau (PSB, the Chinese version of the CBI). During the 2008 Olympics, Western hotel chains were asked to install special Internet monitoring devices that would give the PSB even more access to Internet activities.

The Chinese Internet spy network relies heavily on bots. Many Chinese websites have these embedded bots, and simply logging onto a website could trigger the download of a bot onto the host computer. Given that the Internet in China is centrally controlled by the government, these bots likely are on many common websites, including English-language news sites and expatriate blogs. It is important to note that the Chinese cyber warfare capability is not limited by geography. The government can break into websites anywhere in the world to install bots.

China has invested considerable time and resources to developing its bot armies, focussing on quantity rather than quality and shying away from more creative forms of hacking such as SQL injections (injecting a code to exploit a security vulnerability)[35] and next-generation remote exploits (in such features as chat software and online games). The best thing about bots is that they are easy to spread. An extensive bot army, for example, can be employed both externally and internally, which puts China at a distinct advantage. If Beijing wanted to cut its Internet access to the rest of the world in a crisis scenario, it could still spy on computers beyond its national

35. SQL injection is an attack in which a malicious code is inserted into strings that are later passed to an SQL server for parsing and execution. It is a technique that exploits a security vulnerability occurring in the database layer of an application. In computing, a parser is one of the components in an interpreter or compiler, which checks for correct syntax and builds a data structure (often some kind of parse tree, abstract syntax tree or other hierarchical structure) implicit in the input tokens.

boundaries, with bots installed on computers around the world. The upkeep of the spy network could easily be accomplished by a few people operating outside of China. In comparison, India, because of the myriad operators, does not have the ability to shut down its Internet network in a time of crisis, nor could it get into China's network if it were shut down.

A great deal of the computer chips and other hardware used in manufacturing computers for companies and governments are made in China; and these components often come from the factory loaded with malware.

A bot army might be a large, blunt instrument, but finding a bot on a computer can be a Herculean task, beyond the capabilities of some of the most Internet-savvy people. Moreover, the Chinese have started to make their bots "user-friendly." When bots were first introduced, they could slow down computer operating systems, eventually leading the computer user to reinstall the hard drive (and, thus, killing the bot). Sources say that Chinese bots now can be so efficient they actually make many computers run better by cleaning up the hard drive, trying to resolve conflicts, and so on. They are like invisible computer housecleaners, tidying up things and keeping users satisfied. Since there is no such thing as a free lunch, the payment for this housekeeping, of course, is intelligence.

In addition to bots and other malware, the Chinese have many other ways to expand their Internet spy network. A great deal of the computer chips and other hardware used in manufacturing computers for companies and governments are made in China; and these components often come from the factory loaded with malware. It is also common for USB flash drives and computers to come from the factory preloaded with malware. These components make their way into computers operating in major companies and governments. The Pentagon in November 2008 was forced to ban the use of USB thumb drives because of a computer security incident.[36]

36. Associated Press, "Pentagon Bans Thumb Drives," November 21, 2008, http://www.military.com/news/article/pentagon-bans-thumb-drives.html

NETWORK ATTACKS AGAINST LOGISTICS

Preemption [*xianfa zhiren*] is a core concept of emerging Chinese military doctrine. It is a strategy by which they aim to overcome even a powerful adversary by taking advantage of serious gaps during the deployment stage. By pursuing the strategy of preemption, they endeavour to overcome the enemy by launching preemptive strikes during the early phase of the war or in the preparations leading to the offensive. The Chinese are developing preemption as their core strategy after analysing the operational vulnerabilities of the US during the deployment phase. Using this strategy, they seek to zero in on the hubs and other crucial links in the system that move enemy troops as well as the war-making machine, such as harbours, airports, means of transportation, battlefield installations, and the communications, command and control and information systems. They view India as a slow starter and extremely vulnerable in the initial stages of the conflict. The analysts believe that a preemption of information operations mainly relying on distant battle and stealth to destroy or disrupt C3 systems is the best way to deliver a bolt from the blue in the initial stages of the conflict and seize the initiative. The idea of a preemptive CW/IW strike has been elevated to the central place in the PLA's design of the attack: crippling the enemy's major military assets rather than its urban centres. This has also broadened their vision in waging an anti-Revolution in Military Affairs (RMA) war against a superior opponent.

There are two macro-level targets for Chinese computer network operations: military network information and military information stored on networks. Computer network attack seeks to use the former to degrade the latter. Like the US doctrine, Chinese CNA targeting therefore, focusses specifically on "enemy C2 centres," especially "enemy information systems." Of these information systems, PLA writings and interviews suggest that logistics computer systems are a top priority military target. According to PLA sources, it is essential to zero in on the crucial links in the opponents' apparatus that move enemy troops such as their information systems, and neutralise their information accuracy, timeliness of information, and reliability of information.

In addition to logistics computer systems, another key military target for Chinese CNA is military reliance on civilian communications systems. This view stems from the PLA's analysis that the main US weakness is during the deployment phase, where the US is heavily dependent on computer networks. Chinese authors highlight that the US uses the civilian backbone and unclassified computer networks (i.e., NIPRNET) which are attractive targets and an intelligence goldmine. This is a potential vulnerability which can be attacked through computer network attacks. Classified networks, on the other hand, are an attractive target but could be less accessible.

Computer network attack could also delay resupply to the theatre by misdirecting stores, fuel, and munitions, corrupting or deleting inventory files, and thereby hindering mission capability. The advantages to this strategy are numerous: (1) it is available to the PLA in the near-term; (2) it does not require the PLA to attack/invade any state with air/sea assets; (3) it has a reasonable level of deniability, provided that the attack is sophisticated enough to prevent tracing; (4) it exploits perceived casualty aversion and overattention to force protection; and (5) it overcomes the tyranny of distance and could achieve the desired operational and psychological effects.

THE GENERATION LEAP STRATEGY

Throughout its history, the PLA has suffered from inadequate and outdated information technology, characterised by limited capacity and lack of security. In the past, these weaknesses had severely limited the military's ability to transmit and process large amounts of information or coordinate activities among the various military regions, thereby reducing military effectiveness. The PLA is very much aware of the critical role played by information-based C4ISR technologies in the Gulf and Afghanistan Wars. To overcome these deficits, the PLA has embarked on a well financed generation leap strategy to modernise its infrastructure. The idea of a generation leap is at the core of the PLA's IT-RMA transformation. It means that the PLA pushes two transformations simultaneously: mechanisation and informatisation. In the West, the former precedes the latter, as the platforms are the carriers of the systems. China's mechanisation is far from complete, but it is in a

The transfer of technologies required for leapfrogging in the C4ISR domain was facilitated by the enormous competition amongst the Western telecom firms to get a share of the billions in the potential Chinese market.

hurry – the PLA is trying to invent its own way of informatising.

According to Chinese military analyst You Ji, the PLA is currently engaged – as part of an ambitious "generation-leap" strategy – in a "double construction" transformational effort of simultaneously pursuing both the mechanisation and informatisation of its armed forces. Initially, the PLA intends to digitise and upgrade its current arsenal of conventional "industrial age" weapons – through improved communications systems, new sensors and seekers, greater precision, etc. Concurrently and with equal emphasis, the Chinese are trying to leapfrog development in building informationised capabilities, by putting greater effort and resources into C4ISR infrastructures, networking, and information warfare. By this process, the PLA hopes to transform itself from a mechanised military into a informatised military, with a combat capability for both "soft kill and hard kill." The PLA informatisation can be divided into three stages of evolution: digitalisation, systems integration and intelligentisation (*zhinenghua*). Digitalisation is the initial phase. The PLA has not fully entered this stage, but it is already working on comprehensive networking.

The PLA believes that its late start can save it from the blind exploration of a wrong path. The US experience shows the rules of, and steps in, transformation from mechanisation to informatisation. Through learning from the US, the PLA hopes to skip a few stages of development and enter the fast track early. American military reforms are, therefore, providing a good roadmap for the PLA to quicken the pace of its reforms.

The transfer of technologies required for leapfrogging in the C4ISR domain was facilitated by the enormous competition amongst the Western telecom firms to get a share of the billions in the potential Chinese market. The state backed Chinese IT sector quickly moved beyond merely

importing Western technology to co-developing technology with them. Significant players in the Chinese telecoms market, such as Huawei and Datang, maintain deep co-development relationships with the world's top information-technology powerhouses, but they also have clear ties with the Chinese military, which has now become both a research partner and a valued customer for their IT products.

In microelectronics, China is quickly becoming an important design and production base in the global semiconductor industry, providing the PLA with potential access to a secure supply of advanced integrated circuits for use in sensors and weapon systems. The result is significant levels of military access to cutting-edge information technology, fuelling a C4ISR revolution in the armed forces.

The introduction of an advanced, secure telecommunications infrastructure, has enabled the PLA to achieve significant improvement in its communications and operational security[37], as well as in its capacity to transmit information. The use of advanced optical fibre communications facilities, satellites, long-distance automated switches and computer controlled telephone systems have significantly accelerated the Chinese armed forces' digitisation process and the rapid transmission and processing of military information. The speedy development of strategic communications networks has shortened the distance between command headquarters and grassroots units, and between inland areas and border and coastal areas. Currently the armed forces' networks for data exchange have already linked up units garrisoned in all medium-sized and large cities in the country as well as in the border and coastal areas.

As a result of the automated exchange and transmission of data, graphics and pictures within the armed forces, military information can now be shared by all military units.[38] On the sensor front, China has also made significant advances, as evidenced by the deployment of new constellations of navigation satellites (*Beidou*), communications satellites

37. James C. Mulvenon, "Chinese C4I Modernisation: An Experiment in Open Source Analysis," http://www.rand.org/pubs/conf_proceedings/2005/CF189.pdf
38. Evan S. Medeiros, Roger Cliff, Keith Crane, James C. Mulvenon, "A New Direction for China's Defence Industry," http://www.rand.org/pubs/monographs/2005/RAND_MG334.pdf

The PLA's projection is that in a worst case scenario, China's future war will be fought against lightning air and missile surgical strikes, or sustained air, missile and electronic bombardment.

(*Dongfanghong-4, Fenghuo*)[39], and phased-array radars.[40]

CONCLUSION

The PLA's projection is that in a worst case scenario, China's future war will be fought against lightning air and missile surgical strikes, or sustained air, missile and electronic bombardment. If it is the PLA that takes action, it would be an information dominated attack. Non-personnel engagement will be a new but prominent feature of combat, although exchange of fire within short distances (e.g., aerial dog-fights) could possibly occur.

The idea of a preemptive IW strike has been elevated to the central place in the PLA's design of the attack: crippling the enemy's major military assets rather than its urban centres. This has broadened its vision in waging an anti-RMA war against a superior opponent. To PLA strategists, the informatisation of the US military has not only generated strength, but also exposed weaknesses. The 9/11 tragedy reflects the vulnerability of a mighty nation to new kinds of war. The PLA is contemplating various types of asymmetrical warfare for self-protection. To this end, China is developing new IW measures. Cyber attacks on the enemy's C4ISR will be an integral part of future warfare. Such attacks are much cheaper than attacks on carrier battle groups. The PLA believes that the more a military depends on IT, the more vulnerable it becomes to strikes at its information hubs. For the first time, militarily weaker powers have found the means to deliver punches to the soft-underbelly of the more powerful enemy.

The much talked about missile threat is another form of non-contact warfare the PLA in contemplating. Saturated conventional missile attacks at military targets and communication hubs are one of the first choices.

39. Mark A. Stokes, "China's Strategic Modernisation: Implications for the United States," http://www.fas.org/nuke/guide/china/doctrine/chinamod.pdf
40. *People's Daily* (China), "China's New Missile Destroyer: the 'Magic Shield of China'" http://www.freerepublic.com/focus/f-news/919629/posts

The goal of missile warfare is to bring the war to the enemy's territory. It reduces human losses for the PLA, and has a greater psychological effect on the opponent's population. Missile launches are also more manageable and can be halted promptly to avoid escalation and direct confrontation.

The PLA has been particularly influenced by the information technologies-led RMA and is determined to transform the PLA into a force capable of fighting and winning "limited local wars under conditions of 'informatisation'." This doctrine revolves around short duration, high intensity conflicts characterised by mobility, speed, and long-range attack, employing joint operations fought simultaneously throughout the entire air/space, land, sea and electro-magnetic battlespace, and relying heavily upon extremely lethal high technology weapons.

Consequently, the PLA has in recent years put considerable effort into acquiring new capabilities for mobility, power projection, and precision strike. The PLA has made undeniable progress since the late 1990s in expanding its capabilities in several areas, particularly missile attack, power projection over sea and in the air, space, INEW, directed energy weapons and precision-strike. "Informatisation" is a potentially critical new development in the PLA's war-fighting capabilities, implying a fundamental shift from being platform-centric toward INEW. China's military transformation has, more than any armed force in the Asia-Pacific region, imitated US transformation in terms of ambition and scope. Long-term trends in Chinese military modernisation have the potential to pose a credible threat to militaries in our region if they are not doing so already.