No Contact Warfare and the China Factor

DAVINDER KUMAR

In the aftermath of Desert Strom in 1991, the late Maj Gen Vladimir Slipchenko coined the phrase "*Sixth Generation Warfare*" to refer to the "*Informatisation*" of conventional warfare and the development of precision strike systems, which could make massing of forces in the conventional sense an invitation to disaster and demand the development of the means to mass effects through depth to fight *system versus system* warfare. He had analysed combat experience abroad to further refine his conception until he began to speak of the emergence of "*No Contact Warfare*" as the optimum form of sixth generation warfare. Slipchenko redefined sixth generation warfare as involving the capacity to conduct distant, no contact operations and suggested that such conflict would demand major military reforms. Slipchenko, made a compelling case for the enhanced role of Command, Control, Communication, Computers, Intelligence, Surveillance, Reconnaissance (C4ISR) in conducting such operations.

Definition of No Contact Warfare

The evolution of No Contact Warfare (NCW) has been primarily due to the impact of the media showing the body bags and loss of limbs of young soldiers and the technology making available the means to conduct such warfare. The main motivation is to minimise the casualties and limit collateral damage as a byproduct. The underlying principle of NCW is *"fighting wars without suffering casualties"*.

A broad definition of the term could be: "Type of warfare which involves application of all national capabilities in an integrated manner, while ensuring minimum physical contact of own forces, to conduct distant operations to achieve a quick decisive victory by disrupting, denying and destroying the enemy's war waging potential and his command and control systems through remote delivery of destructive kinetic energy and soft power by relentless Information operations".

The underlying principle of No Contact Warfare is *"fighting wars without suffering casualties"*.

This definition encompasses information warfare/information operations, missile warfare, remote warfare (drone attacks) and robotics in an environment of battlefield transparency and command and control provided by Command, Control, Communication, Computers, Intelligence, Surveillance, Target Acquisition and Reconnaissance (C4ISTAR) systems.

Important Characteristics

NCW, a Domain of Both the Strong and the Weak

Technological superiority in terms of battlefield transparency (C4ISTAR), information operations, precision weapons, command and control systems, long range delivery means like missiles, unmanned platforms and systems [Unmanned Aerial Vehicles (UAVs), Unmanned Combat Aerial Vehicles (UCAVs)], underwater vehicles navigation and tracking systems, both surface and space-based, weather making and forecast systems, robotics, sensors and seekers, and so on, backed by a modern and sophisticated defence industrial base; top of the line Research and Development (R&D) in basic and applied research, and a well informed and determined leadership are considered essential for a viable NCW capability. Ironically, these also make the advanced nations more vulnerable to information operations. These vulnerabilities can be exploited by the weaker nations.

Organisation and Skill Sets

Technological superiority has to be backed by a highly trained and motivated force and a responsive organisation. This requires selection, training, retention and continual upgradation of the resource in consonance with the development and fielding of systems. A great challenge, indeed, considering the variety of skills required and continual training and retention of this resource in service.

Troops on the Ground

NCW will have to be supported by special operations troops on the ground for gathering intelligence, real time surveillance, target designation, damage assessment, information operations, and so on. This is, of course, true only where focussed operations to capture/eliminate enemy or to capture territory for a desired duration are launched.

NCW and Sovereignty

NCW is changing the concept of national sovereignty as is being seen in the drone strikes by the USA in Pakistan, Afghanistan, Libya, Yemen and Tunisia, and the Computer Network Operations (CNO) being conducted by different nations for intelligence gathering, vulnerability assessment, testing of cyber weapons and the response of target nations to such attacks, economic destabilisation, and so on. We will have to wait and see how the international community and the United Nations (UN) react to these happenings.

Power Projection

NCW, through Information Operations (IOs) and long range precision weapons provide a distinct capability of power projection. Interestingly, the IOs provide this capability to weaker nations at a fraction of the cost. No wonder, therefore, that more than 140 nations in the world are busy developing offensive cyber capabilities. One example could be Iran's response to the Stuxnet attack on its nuclear facility by way of a cyber attack on Saudi Arabia's oil facility.

What Are Information Operations?

As seen in the definition, IOs are at the heart of NCW capability. What are IOs and how do they impact NCW?

Definition (as per US Department of Defence)

'Information Operations (IOs) are described as the integrated employment of Electronic Warfare (EW), Computer Network Operations (CNOs), Psychological Operations (PSYOPS), Military Deception (MILDEC) and Operational Security (OPSEC) in concert with specified supporting and related capabilities to influence, disrupt, correct or usurp adversial human and automated decision-making while protecting our own. Inherent in the above definition are the following:

Three Essential Functions of IOs

- Capability to attack the communication networks and electronic systems.
- Recognise the fact that networks are vulnerable and will become more vulnerable as new technologies and functionalities are incorporated.
- Ensure own networks and systems are protected at all times to maintain decision superiority.

Five Core Capabilities

- Electronic Warfare (EW) to include Electronic Support Measures (ESM), Electronic Counter-Measures (ECM) and Electronic Counter Counter-Measures (ECCM).
- PSY OPS
- Operational Security (OPSEC)—this is a process that identifies critical information to determine: if friendly actions can be observed by the adversary's intelligence; if information obtained by the adversaries can be interpreted to be useful to them; and which executes selected measures that eliminate or reduce exploitation of friendly critical information by the adversary. In short, *OPSEC is the process of protecting little pieces of data that could be grouped together to give the bigger picture.*
- Military Deception (MILDEC), both through physical and electronic means. (includes cyber deception).
- Computer Network Operations (CNOs), commonly known as **Cyber/Code War**, to include Computer Network Attack (CNA), Computer Network Defence (CND) and Computer Network Exploitation (CNE).

Five Supporting Capabilities

- Information assurance.
- Physical security.
- Physical attack.
- Counter-intelligence.
- Intelligence, Surveillance, Reconnaissance (ISR) and image analysis capability.

Three Additional Related Capabilities

- Media and public affairs.
- Civil military operations.
- Military support to public diplomacy.

Where Does India Stand?

India has reasonable capabilities and experience in the fields listed above, with islands of excellence in some and a nascent capability in others. In some critical areas like electronic warfare and radars, we have developed indigenous capability for design, manufacture, testing and fielding. We also have experience in conducting PSYOPS as demonstrated in the Punjab, Jammu and Kashmir (J&K) and Northeast (NE) insurgencies.

In the areas of OPSEC, CNO and information assurance, we lack:

- Synergies within various government and intelligence agencies, industry and academia.
- Political will, bureaucratic accountability and timely implementation of policies and projects.
- Timely decision-making.
- The strategic capabilities of joint planning, training and execution.
- Own chip manufacturing facility and 'fabless' manufacturing.
- Indigenous operating software, information security standards.
- Especially skilled manpower in different disciplines and language experts.

ICT Infrastructure

India has a very well developed Information and Communication Technology (ICT) and media infrastructure, both terrestrial and space-based. Internet and TV penetration is one of the highest in the world. India is in the process of establishing a nationwide broad band network for e-governance. It is also developing its physical infrastructure which remains vulnerable to physical attacks through missiles, sabotage and terrorist activities. The degree of automation of India's vital infrastructure like nuclear energy, power grids, airports, air defence, hydroelectric projects, transport sector, finance, banking and health sector is increasing, with attendant vulnerabilities to cyber attacks.

Cyber Security

- A comprehensive National Cyber Security Policy-2013 has been announced recently.
- Formal cyber security responsibilities have been assigned to various organisations but the synergy and organisational effectiveness as on date remain low.

Some salient aspects are:

- CERT-In (Computer Emergency Response Team-India) with the mission to enhance the security of India's information and communication infrastructure through proactive action and effective collaboration
- Standardisation Testing and Quality Certification (STQC) under the Department of Information Technology (DIT) provides assurance services for software quality testing and information security and Information Technology (IT) service management.
- With the help of the industry, the National Association of Software and Services Companies (NASSCOM), a Data Security Council of India has been set up with a mandate to involve the private sector in the area of cyber security.
- The National Technical Research Organisation (NTRO) has been made responsible for overall protection of NII and offensive cyber capability along with the armed forces and the Defence Research and Development Organisation (DRDO).
- The National Critical Information Infrastructure Protection Centre (NCIPC) is being set up along with a centralised ICT command centre for protection of India's ICT infrastructure.
- Further, a National Telecom Network Security Coordination Board (NTNSCB) is being set up to strengthen the national telecom security of India.
- A National Cyber Coordination Centre is to be established.
- A special drive is needed to increase awareness of the vulnerabilities and the associated threats amongst the users.
- Investments in cyber security are low and perhaps insufficient.
- The legal framework in the form of the IT Act 2000, as amended in 2008, exists. Implementation, however, is poor at present.
- Security consciousness and cyber discipline amongst users is poor.
- Indigenous hardware and cyber security software is almost non-existent, resulting in enhanced vulnerability. Concerted efforts are required to manage the risks in the supply chain management—this is a strategic requirement.
- Adequate international tie-ups and more alliances are needed, with active participation in the Internet governance mechanism.
- The procurement procedures are cumbersome, hence, there is very poor implementation on the ground.
- Reporting of cyber incidences to CERT–In is poor
- Network audit, vulnerability assessment and gap analysis are poor.

- Indigenous cryptography for use by citizens, financial institutions and industry is yet to be developed and fielded.
- Awareness, drills and procedures for risk management need improvement.
- There is low skill set availability for cyber security and language experts—596 in India, approximately 7,500 more approved for induction, with 1,200 for the defence forces) against 1,93,000 in China and 80,000 in the USA. The cyber security policy envisages availability of half a million cyber security experts in the next 3-5 years—a herculean task indeed.
- Data management and data security is high in the data centres, medium in the industry and low in the government.
- Cyber security standards are yet to be promulgated.

C4ISR, Space and Missiles

In the field of C4ISR, India has made some progress but a lot still needs to be done, particularly in the higher defence organisation, jointmanship, information management to include secure storage, analysis and transmission, sharing of information within the Services and the government; development of indigenous capability in the fields of semi-conductors, standards and testing, manufacturing, system integration, cryptography, image processing, and so on. The speed of decision-making, and synergy and accountability need improvement.

India is progressively building capability in battlefield transparency to include all weather satellites, UAVs, Airborne Warning and Control System (AWACS), Airborne Early Warning (AEW) aircraft, aerostats, Electronic Intelligence (ELINT) and Signals Intelligence (SIGINT) assets, P-8i long range maritime surveillance aircraft, long range coastal radars, and so on. It has done well with regard to navigation and target acquisition, through both developing indigenous capability by way of the Indian Regional Navigation System (IRNS) as also by information and resource sharing agreements with Global Positioning System (GPS) providers like NAVSTAR of the USA, GLONASS of Soviet Russia and Galileo of the European Union.

As regards satellite design, launch vehicles and telecommand and telemetry systems, India has done well. Indian satellites have been launched using US, Russian and European launch vehicles, giving substantial system integration experience. India has successfully demonstrated the Multiple Advanced Reentry Vehicle (MARV) system, multiple satellite launch on a single vehicle, and launching of nano and pico satellites. With the recent successful launch of the Geosynchronous Space Launched Vehicle (GSLV) with an indigenous cryogenic engine, India has entered the elite club of nations having such a capability and would soon be in a position to launch heavier satellites.

In the areas of missiles, again we are progressing with the Prithvi, Agni series, BrahMos and Nirbhay cruise missiles on different platforms. The Defence Research and Development Organisation (DRDO) has technically demonstrated both the exothermic and endothermic ballistic missile defence capability. The previous DRDO Chief is on record to state that with the successful launch of the Agni-5, India has all the components of a viable Ballistic Missile Defence (BMD) capability, as also the capability to launch low earth satellites in case of an emergency/urgency.

China is preparing for full spectrum warfare wherein all organs of government will get involved.

The China Factor

Since 1970, China has been engaged in the systematic modernisation of its defence forces. The modernisation encompasses change in doctrine, induction of new weapons, platforms and systems based on advanced technology, organisational transformation, training and technology required to become self-reliant, and establishment of a very strong defence industrial base. The People's Liberation Army (PLA) has reduced its manpower and deployed modern systems in its land, air, sea and missile forces. This has led to increase in the PLA's overall military effectiveness, especially in the context of local war under conditions of *informationisation.*

China has assessed and analysed the strength and vulnerabilities of its likely adversaries, mainly the USA, and tailored its approach to both negate their strengths and exploit their vulnerabilities. Backed by rapid economic growth, it has concentrated on the strategic areas of space, nuclear, missile and information warfare capabilities with '*mechanisation*' and '*informationisation*' being at the core. India's doctrine of Integrated Network and Electronic Warfare (INEW) as modified by the "system of systems" concept *of information confrontation,* supports kinetic warfare and information warfare which includes cyber warfare, electronic warfare, psychological warfare, and space and nuclear warfare; and it has selectively concentrated on 'lead ahead' capabilities in niche areas like C4ISR, aviation and space.

Key Capabilities

The PLA today is entering its second decade of a sustained modernisation drive that has generated remarkable transformation within the force. While the modernisation of China's military hardware continues to capture headlines, the rapid development of a comprehensive C4ISR infrastructure, linking platforms, personnel, and operations, is arguably the most transformative of all PLA efforts currently underway.

China is preparing for full spectrum warfare wherein all organs of government would get involved—some like CNO and political warfare could begin much before the commencement of active hostilities and continue till much after the termination of hostilities. Legal warfare, public opinion warfare and perception management along with information confrontation assets would be employed in an integrated manner with the kinetic means available at its disposal. Considerable importance is being given to self-sufficiency through a very well developed defence manufacturing infrastructure and focussed R&D by involving the private industry and academia. The recruitment policies and training strategies are being modified continuously to get the human resource with the requisite skill sets.

China has the most active and diverse ballistic missile development programme in the world. It is developing and testing offensive missiles, forming additional missile units, qualitatively upgrading certain missile systems, and developing methods to counter ballistic missile defences. China's ballistic missile force is expanding both in size and types of missiles. BMD counter-measures, to include the Multiple Independently Targeted Reentry Vehicle (MIRV) and MARV payloads, decoys, chaff, jamming and thermal shielding are all under active development.

China may use CNE operations designed purely for reconnaissance purposes to map our network topologies and understand their relationship with the command and control structure. Such reconnaissance conducted during peace-time can support offensive operations during a war.

CNE can also be used during peace-time to install malware which can provide intelligence during peace-time and can be triggered during a war to cause damage or disruption. The Chinese operators could create intentional 'noise' on the networks that elicits an Indian reaction, thus, enabling the attackers to gather intelligence on how the Indian defence posture will change under such circumstances.

There is a definite political will in China towards developing capabilities for fighting a war in the 21st century and claiming the top slot amongst the comity of nations. India would need to do a lot more to match and possibly catch up with those capabilities.

Lt Gen **Davinder Kumar** is a former SO-in-C.

References

1. "Russian Sixth Generation Warfare and Recent Developments," Startrisks.com/geostrar/3739
2. "What Are information Operations ?," www.au.af.mil/info-ops/what.htm
3. National Cyber Security Policy-2013.
4. Glimpses of Indian Space Programme—ISRO, www.isro.gov.in/publications/pdf/glimpses of indian space programme.pdf
5. Integrated Guided Missile Development Programme, en.wikipedia.org/wiki/integrate_guided_missile_development_programme
6. Indian Ballistic Missile Defense Programme, en.wikipedia.org/wiki/indian_ballistic_missile_defense-programme
7. "Chinese Capabilities for Computer Network Operations and Cyber Espionage,"pdf
8. "Chinese Military and Force Development," July 2012.
9. "China: On March to Virtual Conflicts."
10. "China has World's Most Active Missile Programme," www.bloomberg.com
11. "China Persues Systems to Keep US Dorces at Bay," www.defensenews.com/article/20130917/DEFREG03
12. "Chinese Missile Ranges," *Economist,* www.economist.com/blogs/daily chart/2010/12