Securing the Cyberspace

Kamal Davar

The four dimensions of modern warfare in the realms of land, sea, air and space have further expanded with the dawn of the age of information warfare (IW), further complicating the myriad forms of modern conflict. IW has accentuated like never before, not only asymmetric warfare, as commonly understood, but a war which knows no boundaries, in which it is problematic to trace the origins of the attackers, and which does not even require a conflict situation and can be easily waged 24/7 even in times of peace. Information or cyber warfare can win battles without crossing borders and can neutralise diverse capabilities of potential adversaries well before the onset of battle, if required.

Cyber crimes are unlawful acts wherein a computer is either a tool or a target or both. Cyber warfare, the new bloodless war zone, simply put, is the use of information technology (IT) and computers to undertake hostile actions or acts of war against target governments and their sensitive agencies, offices, armed forces, large commercial organisations, or other national entities like the power grids, aviation and railways sectors or stock exchanges and banking systems. It is an attack on information in the information age, primarily undertaken to acquire knowledge of a potential adversary and gain control over his vital and sensitive information to degrade or destroy his capabilities by infecting his computers with 'viruses' and electronic messages. The initiator of cyber warfare can either be an individual, a group, an agency or a government and with the rapid spread of IT, cyber threats may now originate from both state and non-state actors, obscuring the identity of the initiator.

Cyber warfare could take the form of specialised hacking jobs on a specific server to generate targeted denial of service attacks. A well orchestrated cyber attack can ensure the target being deprived of its ability to connect or share vital information with its other stakeholders on the internet, and in worst cases,

Lieutenant General **Kamal Davar** (Retd) is former Director General, Defence Intelligence Agency.

result in an electronic paralysis of essential services in an information driven society or organisation, thus, causing unimaginable havoc. The military, now heavily dependent on computers for its command and control architecture, communications, surveillance and early warning systems, precision targeting, data bases, and above all, speedy and instant dissemination of orders and instructions and sharing of vital data with its formations and units, is now very vulnerable to electronic and cyber attacks from rogue hackers and adversaries during critical engagement and decision-making cycles.

There is no exaggeration in stating that the world now acknowledges the formidable cyber threats emanating from the 'all weather friends', China and Pakistan. The Chinese have successfully hacked, for years, sensitive US websites of the White House, Pentagon, National Aeronautical Space Agency (NASA), nuclear weapons' labs, and many of its big corporations, apart from others. As also commonly known, since the Pokhran II tests in 1998, Pakistani computer hackers called Milworm and others have been regularly attacking Indian websites like the prime minister's office, national security adviser's office, the Bhabha Atomic Research Centre, some security agencies, the Videsh Sanchar Nigam and other telecom companies, and the Indian Science Congress website, and have defaced them with anti-India obscenities. Pakistani hacker groups like Death to India, Kill India, and G-Force Pakistan, openly circulate instructions for attacking Indian websites. Whether these highly illegal acts are the handiwork of Pakistani amateurs or of Pakistani intelligence agencies or groups trained and sponsored by them has not been conclusively proved. It is also of concern that certain Islamic terror groups have now acquired expertise in IW skills. The RAND Corporation has recently opined that, "Osama bin Laden's Egyptian followers can immediately cripple the information infrastructures of Russia and India." A report titled "Shadows in the Cloud", from the Canada based Munk Center for International Studies in Toronto University, states that a China-based cyber spy network has been targeting the Indian military.

Some Indian experts have pointed to a command and control system, set up by a core of servers in Chengdu and Hainan provinces in China, that uses free web-hosting services and social networking sites like Twitter and Google to manipulate accounts. According to a reputed military journal, *The Indian Military Review's Report*, published last year, a large number of websites at many Indian diplomatic missions abroad were also compromised. In addition, the report also suggests that computers in the National Security Council Secretariat were also infected, "giving the hackers access to confidential documents on

the security assessment of the northeastern states and the Naxalite movement, besides information on missile defence systems and military equipment." The Dalai Lama's office in Dharamsala is also regularly targeted. This cyber espionage operation, brought to light in 2009 by the Information Warfare Monitor and dubbed 'Ghost-Net', is widely believed to having been undertaken by Chinese operatives. What is, thus, known to the Indian establishment may just be the tip of the iceberg and the exact dimensions of the damage being caused to Indian security may never be gauged. Reportedly, the Indian government's premier National Informatics Centre (NIC), which controls all governmental websites, was also infected for some time.

By all standards, China poses a greater cyber threat than Pakistan and Islamic terror groups. According to the US Army's Foreign Military Studies Office in Fort Leavenworth, Kansas, China's leadership surmises that it can achieve its manifold objectives in Asia only by integrating information warfare into its geo-political strategies—coupling the latest information warfare techniques into its people's war concepts. It opines that "this development has been ignored by the West but will have far-reaching strategic and operational implications." It may be recalled that in mid-1999, China had established a special task force on information warfare consisting of senior politicians, academics and military officers. Reportedly, this task force prepared detailed plans to cripple the information structures of Taiwan, the USA, India, Japan and South Korea. China's People's Liberation Army (PLA) has been conducting several field exercises to hone its information warfare skills. Simulated cyber attacks, on target countries, have been practised which include planting information mines, conducting information reconnaissance, changing network data, releasing information bombs, dumping information garbage, applying information deception, disseminating propaganda, organising information defence, establishing network spy stations, etc. Demonstrations for the top political and military leadership, including the Beijing Military Command, Central Military Commission and the General Staff Directorate, to showcase their information warfare skills, have been periodically undertaken. Way back in 2007, Gen James Cartwright, chief of the US Strategic Command, in his testimony to the US Congress, had accepted that "already America is under widespread attack in cyberspace and some of these attacks had reduced the US military's operational capabilities." It will be interesting to note that the US Air Force has had information warfare squadrons since early 1980s. In fact, the official mission of the US Air Force currently stands as, "to provide sovereign options for the defense of the United States and its global interests, and to fly and fight in Air,

Space and Cyberspace," with the latter alluding to its IW role.

Air forces, the world over, often risk aircraft and aircrews to attack the enemy's strategic communication targets and early warning systems. Remotely degrading and disabling such targets using software and other IT means provides a safer and more cost-effective alternative, rendering them ineffective by electronic means instead of explosive means! Countless operational applications for the other two Services similarly exist, provided adequate IT defensive measures are in place which cannot be degraded by the enemy.

Suggested Indian Response to IW Threats

It is but natural that as an emerging power with a vibrant growing economy, India will be relying increasingly on its support systems, national entities, infrastructure, both civil and military, on automation and network-centricity. With China and Pakistan and now even some non-state actors targeting India's systems in myriad diabolical ways, the Indian establishment along with its IT supported sectors must fully comprehend the perils of the Information Age and the inescapable imperative to protect its systems, infrastructure and its core civil sectors, and, importantly, its security architecture. The vulnerability that our systems have shown in the past decade to the machinations of these hackers, calls for an urgent look inwards to put into place both defensive and offensive capabilities to thwart the evil designs of our adversaries. Seized with the seriousness and enormity of the cyber threats, Defence Minister A K Antony had exhorted the Services' top brass at the Unified Commanders Conference, in April 2010, to synergise their expertise to meet the challenges of cyber warfare. A suggested Indian response to meet the IW threats is given, briefly, as under:

- A comprehensive, all encompassing, National Strategy for Information and Cyber Security to be conceived, formulated and implemented by all stake-holders in the country. The IT Act 2000 to be updated to address cyber crimes and cyber terrorism.
- India needs to take the lead in the UN to make world organisations formally take cognisance of cyber crimes and cyber terrorism. The world endeavours to take punitive measures including economic sanctions against nations indulging in cyber crimes and related offences. The National Technical Research Organisation (NTRO), Defence Research and Development Organisation (DRDO), and the Defence Intelligence Agency (DIA) need to synergise various aspects of IW.

- A central nodal agency to be established to implement the above mentioned national strategy on IT and IW. This could be under the national security adviser and coordinate and synergise the expertise and requirements of all national stakeholders in this field.
- The armed forces could consider setting up an Inter-Services Cyber Command under the Integrated Defence Staff, with DIA coordinating the defensive and offensive IW needs of the three Services.
- Indian software manufacturers must cooperate with governmental agencies to ensure that IT products and services meet the nation's stringent security requirements. All efforts should be made that when hardware or software has to be imported, a security audit is carried out to prevent any mischief by countries or manufacturers using spyware or malware embedded into these imported products. Thus, a National Testing Facility under the DRDO could be considered.
- Ethical hacking by experts on own sensitive systems by simulated cyber attacks to be periodically carried out to check the security preparedness of own networks.
- Adequate numbers of skilled and well equipped Computer Emergency Response Teams for the various sectors should be put in place to handle emergencies in these different entities.

Conclusion

Since the last few years, the world over, the security landscape has dramatically changed from the physical, giving a lot of space to the digital, with myriad unknown but very formidable challenges which can cause untold havoc in the day-to-day life of nations .Today, a nation's capability to successfully withstand the challenges of IW, in peace and war, has become an essential ingredient in measuring its Comprehensive National Power (CNP). As in many fields of military endeavour, China has had a head start and India, though a software giant, needs to catch up speedily in this latest form of civil and military rivalry.