India- One Million Laptop Warriors: China's Emerging Cyberwar Doctrine

Gurmeet Kanwal, Director, Centre for Land Warfare Studies, New Delhi.

In alarming front page news reports published by several Indian newspapers in 2009 and 21010, Chinese cyber spies were reported to have hacked into computers and stolen documents from hundreds of government and private offices around the world, including those of the National Security Adviser and the Indian embassy in the US. Earlier it had been reported that the Chinese army uses more than 10,000 cyber warriors with degrees in information technology to maintain an e-vigil over China's borders. "Chinese soldiers now swipe cards and work on laptops as they monitor the border with great efficiency… electronic sentinels functioning 24 hours a day." This number will soon go up to one million laptop warriors.

While information about the People's Liberation Army's (PLA) cyber warriors has begun to appear in the public domain only recently, PLA watchers across the world have known for long about China's well conceived doctrine on information operations and cyberwar. China's cyberwar doctrine is designed to level the playing field in a future war with better equipped Western armed forces that rely on Revolution in Military Affairs (RMA) technologies and enjoy immense superiority in terms of weapons platforms and intelligence, surveillance and reconnaissance (ISR) and command and control networks.

Early in the first decade of the new century, China's Central Military Commission (CMC) had called for a detailed study of the concept of "people's war under conditions of informationisation", implying increasing attention to the application of information technology to the conduct of conventional conflict. Since then the scope of the cyber war doctrine has been expanded to develop the capabilities necessary to take control of all the major networks that drive the world's economic engines such as banking, stock exchanges and telecommunications if it becomes necessary.

Analysts of the People's Liberation Army (PLA) have called the ongoing Revolution in Military Affairs (RMA) an informationised military revolution with Chinese characteristics. Informationisation relates to the PLA's ability to adopt information technologies to command, intelligence, training and weapon systems. The PLA is seeking to contest the information battle space with its space-based, airborne, naval and ground-based surveillance and intelligence gathering systems and its new anti-satellite, anti-radar, electronic warfare and information warfare systems. According to China's White Paper on National Defence issued in 2004, "In its modernisation drive, the PLA takes informationalisation as its orientation and strategic focus."

The denial of information, strategic deception and the achievement of psychological surprise have for long been an integral part of Chinese military doctrine. The Chinese find information warfare (IW) extremely attractive as they view it as an asymmetric tool that will

enable them to overcome their relative backwardness in military hardware. The Chinese are devoting considerable time and energy to perfecting the techniques of IW to target the rapidly modernizing Western armed forces that are becoming increasingly more dependent on the software that runs computer networks and modern communications. In Chinese thinking, IW presents a level playing field for projecting power and prevailing upon the adversary in future wars.

Information warfare includes intelligence operations; command and control operations to disrupt enemy information flow; electronic warfare by seizing the electromagnetic initiative through electronic attack, electronic protection and electronic warfare support; targeting enemy computer systems and networks to damage and destroy critical machines and networks and the data stored on them; and, the physical destruction of enemy information infrastructure through the application of kinetic firepower. The Chinese call their pursuit of information warfare and other hi-tech means to counter the overwhelmingly superior conventional military capabilities of the Western Alliance "acupuncture warfare". Acupuncture warfare (also called "paralysis warfare") is described as "Paralysing the enemy by attacking the weak link of his command, control, communications and information as if hitting his acupuncture point in *kung fu* combat."

In another five to 10 years China will develop much greater depth and sophistication in its understanding and handling of information warfare techniques and information operations. With Indian society becoming increasingly dependent on automated data processing and vast computer networks, India will also become extremely vulnerable to such information warfare techniques. The fact that it can be practiced from virtually any place on the earth even during peacetime makes acupuncture or paralysis warfare even more diabolical. India can ill-afford to ignore this new challenge to its security.

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

On June 23, 2009, Robert Gates, then US Secretary of Defence, authorised the creation of a new military command that will develop offensive cyber-weapons and defend command and control networks against computer attacks. India too needs a Cyber Command to lead efforts within the military to safeguard computer networks from hackers and cyber attacks.

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

This is too important a field to allow the traditional Indian approach – digging heads into the sand while waiting for the threat to go away – to hold sway and react only when the enemy has reached Panipat and is knocking on the gates of Delhi. In this case, the nothingness of cyberspace connects China's one million laptop warriors directly with Delhi, Mumbai,

Kolkata, Chennai, Bangalore and Hyderabad and other Indian cities, as also India's strategic establishments.

(Gurmeet Kanwal is Director, Centre for Land Warfare Studies, New Delhi.)