Counter China's Laptop Warriors

GURMEET KANWAL
The Economic Times

Former national security adviser M K Narayanan had told The Times, London, before laying down his office that China's cyber warriors had hacked into computers in the PMO on December 15, 2009. At least 30 computers may have been penetrated. Last year, Chinese cyber spies were reported to have broken into and stolen documents from hundreds of government and private offices around the world, including those of the Indian embassy in the US.

The Chinese army uses more than 10,000 cyber warriors with degrees in IT to maintain e-vigil on China's borders. On June 23, 2009, the US secretary of defence Robert Gates had authorised the creation of a new military command that will develop offensive cyber-weapons and defend command and control networks of the US armed forces against computer attacks.

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.

Soon after the Gulf War in 1991, 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 IT to the conduct of conventional conflict.

Since then, the scope of the cyberwar doctrine has been expanded to develop capabilities necessary to take control of all major networks that drive the world's economic engines such as banking, stock exchanges, power distribution, transportation and telecommunications if it becomes necessary. People's Liberation Army (PLA) analysts have called the RMA an informationised military revolution with Chinese characteristics. The PLA is seeking to contest

the information battle 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 (IW) systems.

According to China's White Paper on National Defence, "In its modernisation drive, the PLA takes informationisation as its orientation and strategic focus." Denial of information, strategic deception and psychological surprise have for long been an integral part of Chinese military doctrine. The Chinese are devoting considerable time and energy perfecting IW techniques to target the western armed forces that are becoming increasingly dependent on the software that run computer networks and communication.

The Chinese call their pursuit of IW and other hi-tech means to counter the overwhelmingly superior conventional military capabilities of the western alliance 'acupuncture warfare'. Acupuncture — or 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 5-10 years, China will develop greater depth and sophistication in its understanding and handling of IW techniques and information operations.

With Indian society increasingly dependent on automated data processing and vast computer networks, India is vulnerable to such IW techniques. The fact that it can be practised from virtually any place on earth even during peacetime makes acupuncture warfare even more diabolical. India can ill-afford to ignore this new challenge to its security. India should adopt an inter-ministerial, inter-departmental, inter-services, multi-agency and multi-disciplinary approach to dealing with emerging cyber warfare threats. Since no single agency is charged with ensuring cyber security, a nodal agency must be created to spearhead India's cyberwar efforts under a national cyber security adviser who should report directly to the NSA. The armed forces must be part of the national effort from the beginning so that emerging tactics, techniques and procedures can be incorporated into doctrine and training.

A twin-track strategy must be followed: defensive to guard India's vulnerable assets, such as military command and control networks and civilian infrastructure dependent on the use of cyberspace, as well as offensive to disrupt the adversary's command, control, communication, computers, intelligence, information, surveillance and reconnaissance (C4I2SR) systems, and develop leverages that can be exploited at the appropriate time. With some finest software brains in the world available to India, it should not prove to be an insurmountable challenge. As for vulnerable computers like those in the PMO and the armed

forces headquarters, the only fail-safe option is to ensure that none of them is connected to the internet.

This is too important a field to allow the traditional Indian approach — digging heads in the sand while waiting for the threat to go away — to hold sway and react only when the adversary has reached Panipat and is knocking on the gates of Delhi. In this case, the nothingness of cyberspace connects China's laptops warriors directly with Delhi, Mumbai, Kolkata, Chennai, Bangalore and Hyderabad and other Indian cities, as also India's strategic establishments.

Source: http://economictimes.indiatimes.com/articleshow/5649399.cms