Spy Game
India Readies Cyber Army to Hack into Hostile Nations' Computer Systems

HARSIMRAN SINGH & JOJI THOMAS PHILIP ➤ August 6, 2010
The Economic Times

Borrowing a page from China's art of cyber war, the government is giving shape to an IT infrastructure setup manned by a small army of software professionals to spy on the classified data of hostile nations by hacking into their computer systems. IT workers and ethical hackers who sign up for the ambitious project will be protected by law, says the proposal being discussed by senior government administrators. The expertise of these professionals will be used to go on the offensive or preempt strikes by breaching the security walls of enemy systems. The strategy of taking the fight to hackers was drafted at a high-level security meet on July 29 chaired by National Security Advisor Shiv Shankar Menon. The meeting was attended by the director of Intelligence Bureau as well as senior officials of the telecom department, IT ministry and security agencies, documents seen by ET show. Departments whose officials were present at the meeting did not respond to ET emails. The government is worried about spying and sabotage from neighbouring countries, particularly China and Pakistan, after a spate of assaults on its computer systems in recent times. The Citizen Lab at the University of Toronto said in April that a clique of hackers based in China had conducted extensive spying operations in India, pilfering confidential documents from the defence ministry. Though Beijing strongly denied any role in the attacks, the investigation pointed to the Chinese government's tacit approval of the spying operations. The technical reconnaissance bureau of the People's Liberation Army that is responsible for signals intelligence collection is headquartered in Chengdu, where the hackers had set up base. According to the government proposal, the National Technical Research Organisation (NTRO) along with Defence Intelligence Agency (DIA) will be responsible for creating cyber-offensive capabilities. NTRO is a key government agency that gathers technical intelligence

while DIA is tasked with collating inputs from the Navy, Army and Air Force. The NTRO will also suggest measures to ensure legal protection to recruits, a move that is expected to coax software professionals into joining the government group because under the Indian IT Act, hacking is punishable with imprisonment up to three years, or carries a fine up to `2 lakh, or both. "Even if the offense is done on a computer on foreign soil, it is punishable under Indian laws," says cyber lawyer Pavan Duggal, adding that the IT Act will have to be changed for "patriotic stealth operations". Mr Duggal welcomed the efforts to establish a hacker group, pointing to the explosive growth in assaults on Indian systems recently. Last year, 600 computers belonging to the external affairs ministry were hacked, allegedly by Chinese groups. The hackers also managed to steal crucial documents from the computers of the defence establishment then. Vikas Desai, lead technical lead of network security firm RSA, said the government's efforts can be classified as ethical hacking. "Many countries and organisations in the world already have this kind of infrastructure," he said. In sheer numbers at least, recruitment may not be a problem. The country is due to produce nearly 5.71 lakh technical graduates and postgraduates in 2010, says IT lobby group Nasscom. There is also a teeming workforce in India thanks to large anti-virus and software companies such as McAfee, Microsoft, Intel establishing R&D labs here. The government is not taking chances, however. The NSA's National Security Council Secretariat has directed the HRD and IT ministries to introduce cyber security in the curriculum of IITs and education institutes. The government also plans to amplify efforts to strengthen its cyber armour. A National Testing Centre to check all types of hardware and software being sourced by departments for spyware will be established to prevent India's computers from coming under attack. The NSA has also asked the Defence Research & Development Organisation (DRDO) and DIA to magnify efforts against electromagnetic-pulse bombs that can interrupt wireless signals inside the country. It has also directed the DIA to harden its Transient ElectroMagnetic Pulse Emanations Standards, known as TEMPEST in military parlance. Hardening TEMPEST to a geek means lowering the chances of interception of data transferred by defence agencies on the internet. To enable this, the government wants to involve engineers and scientists from the IITs and Indian Institutes of Science to develop highly-encrypted algorithms, in large numbers. The high-level meeting notes that government's cyber efforts are stumped by its ability to produce no more than 3-4 such algorithms in a year.

Source: http://economictimes.indiatimes.com/articleshow/6258977.cms?prtpage=1