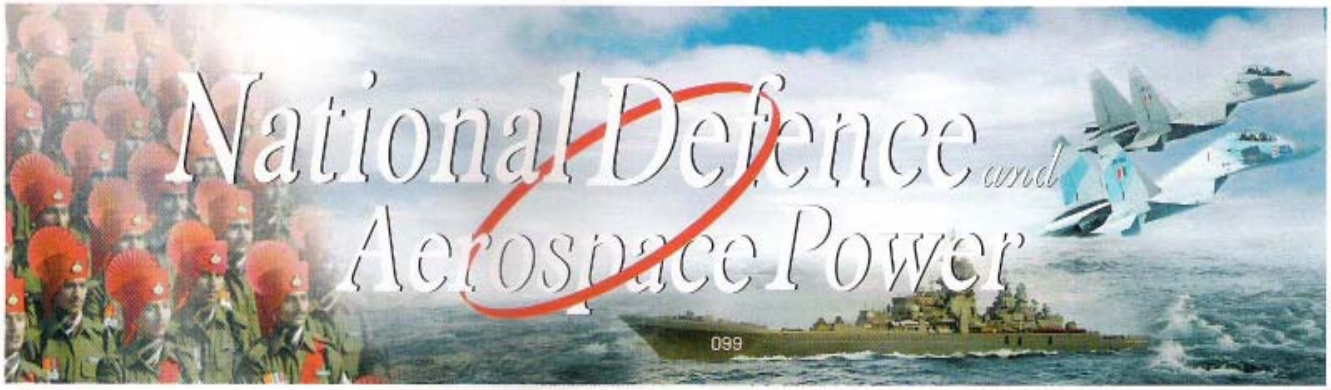

Centre for Air Power Studies ISSUE BRIEF

22\10 1 March 2010

CHINA AND THE LATENT CYBER THREAT

Jayadeva Ranade

Distinguished Fellow, Centre for Air Power Studies, New Delhi

China's cyber capability came into sharp focus again recently when a report, issued coincidentally at the start of SM Krishna's maiden visit to China as Foreign Minister, publicized that Chinese hackers had accessed and 'stolen' voluminous classified information from computers in sensitive government offices in India.

The report, entitled 'Shadows in the Cloud' issued on April 6 by the Munk School of Global Affairs of the University of Toronto jointly with other organisations, stated that a number of computers in Indian establishments had been compromised. Launched specifically to investigate the extent of penetration by Chinese hackers of computers in the Dalai Lama's offices, researchers detected that computers in ten Indian Embassies including Afghanistan, Germany, Italy, Russia, UAE and USA, and the Indian High Commissions in Nigeria and the UK had been compromised. Sensitive establishments targetted included the National Security Council Secretariat (NSCS), a couple of MES establishments, the 21 Mountain Artillery Brigade, two Air Force Stations, the Army Institute of Technology, Pune, the Military College of Electronics and Mechanical Engineering in Secunderabad and the New Delhi Railway Station. Computers of defence-related think-tanks, like the Institute of Defence Studies and Analyses (IDSA) and of academics and journalists working on defence issues were compromised.

Cyber warfare is ideally suited to asymmetric warfare as it affords stealth, speed and deniability and would be the preferred weapon of a weaker adversary.

In March 2009, the Munk Centre and two researchers from the University of Illinois (USA) and Cambridge (UK) had separately issued similarly disturbing reports highlighting China's cyber activity. Those reports revealed that 1295 computers in 103 countries were affected. Many computers were high value targets belonging to foreign governments and the Dalai Lama's offices. Computers in the Indian Embassy in Washington, UK, US, Germany, Serbia, Cyprus, Belgium, Italy, Kuwait and Zimbabwe were identified as affected. Computers in many South East Asian capitals were infected as were others in the Foreign Ministries in Iran, Brunei, Bangladesh, India and Indonesia. The infected node stretched in an arc encompassing India, Bhutan, Bangladesh, Vietnam, Laos, Brunei, Philippines, Hongkong and Taiwan.

All the reports identify China as the source of the cyber attacks. The latest report identifies at least one hacker as based in Chengdu, capital of China's Sichuan province and as associated with officially-tolerated hacker organizations like NSFocus and Eviloctal. Both these outfits, incidentally, have links to the People's Liberation Army (PLA). Another hacker was linked to the University of Science and Technology in Chengdu.

The findings of these reports, along with other independent reports, confirm that India is being subjected to sustained cyber attacks. Selection of the New Delhi Railway Station shows that public utilities are also being targeted. Informed estimates are that the incidence of cyber attacks was quite high last year. Additionally, computers of specific officials in sensitive establishments have been targetted, indicating that a large number of computers were surveilled before a particular target was determined.

The reports are particularly disturbing since China views cyberspace as the battleground of the future. The military dimension to China's cyber technology policy was publicly enunciated in a quasi-official book published in 1999, by two PLA Senior Colonels and entitled 'Unrestricted Warfare'. Cyber warfare is ideally suited to asymmetric warfare as it affords stealth, speed and deniability and would be the preferred weapon of a weaker adversary. Especially in advanced nations like the US, the internet is a critical part of the operating infrastructure of public utilities like water works and electricity grids,

transportation networks, financial institutions, health services, etc. After Hu Jintao, Chairman of China's Military Commission, in 2007 stressed the importance of cyber capability, or 'informationisation' of the armed forces, this became an area of intensive research and capital investment.

The PLA has, since 2002, steadily augmented its cyber force by creating cyber-capable Information Warfare (IW) militia units. Distinction between the civil and military has been deliberately blurred and militia units comprise personnel from the commercial sector and academia.

China formulated its overarching cyber strategy encompassing civil and military applications in the early 1990s. The objective was to secure and control assured supplies of scarce essential resources, acquire dominance in the manufacture of hardware, gain the lead in cyber and wireless technology, and achieve indigenous capability and sophistication in software design. It declared rare earth metals a secret national priority in the mid-1980s. These metals are irreplaceable and used in hundreds of technologies ranging from mobile phones, BlackBerrys, low-light energy bulbs, lasers, missile guidance systems and superconductors to computer hard-drives. In 1997, Deng Xiaoping observed that 'China would be for rare earth metals what the Middle East is to oil' and within twenty years China acquired virtually monopolistic control over their supply. China's Ministry of Industry and Information Technology demonstrated this recently when it proposed a total ban on the export of certain rare earth metals and recommended limiting the export of others to 35,000 metric tonnes a year. Japan, which alone needs over 38,000 metric tonnes each year, has accused China of treating rare earth metal exports as a '21st century economic weapon'.

The PLA has, since 2002, steadily augmented its cyber force by creating cyber-capable Information Warfare (IW) militia units. Distinction between the civil and military has been deliberately blurred and militia units comprise personnel from the commercial sector and academia. Militia units are being created within Chinese hi-tech and Information Technology commercial entities so that trained, technically qualified individuals with advanced education in software design are available. Chinese nationals are being trained in cyber-warfare, many in academies run by the PLA, like the 'informationisation' military courses offered in Wuhan University. While details are obviously not publicized, a few examples discerned from the official Chinese media were included in a report released by the Northrop Group of the US. It cited the case of a Political Commissar of the Guangzhou People's Armed Police Force garrison advocating, in 2003, the direct involvement of urban militia units in information warfare, electronic warfare and psychological warfare. He proposed making information warfare one of the primary missions of the Guangzhou Militia. In 2004 a Tianjin-based militia garrison restructured its subordinate units and created a dedicated 'Information Operations' unit. In 2007, militia units subordinate to a Henan Province military sub-district were organized for communications and network warfare and a year later, in 2008, an Anhui Province militia unit recruited personnel from large private enterprises for specialized technical training. In March 2008, a militia battalion in Yongning County in Ningxia Province, within the operational jurisdiction of the Lanzhou Military Region, established an Information Warfare Group. The Lanzhou Military Region, incidentally, has a support and reinforcement role in military operations against India. Recent reports suggest that it now has an active role in India's western sector in event of conflict with India. This Information Warfare Group was tasked to conduct network warfare research and training and to "attack the enemy's wartime networks". This information was posted on the unit's website on March 19, 2008. The Yongning unit comprises an information warfare centre detachment, information gathering detachment, and a militia network protection unit. The unit is equipped to tackle the entire range of Computer Network Operations (CNO) missions. In February 2009, a PLA television programme publicized that a Division in the Lanzhou Military Region conducted an 'opposed informationisation warfare' exercise featuring computer network attack and defence scenarios while countering electronic warfare attacks, a common feature of informationised warfare training.

The PLA has six Technical Reconnaissance Bureaus (TRB) in the Lanzhou, Jinan, Chengdu, Guangzhou and Beijing Military Regions, which are responsible for SIGINT and computer network operations (CNO). Indications are that the TRB included Information Warfare (IW) in their tasks around 1997. The First TRB in Chengdu, for example, received a series of commendations for 'substantial achievements' in 'informationisation building'. The Chengdu Zhangji Bao on August 20, 2007 reported that Chengdu Military Region Unit 78006 was praised for breakthroughs in 'cutting edge IT research'.

Official US estimates in 2008 noted that Chinese hackers mainly targetted US defence computers and systems and downloaded 10 - 20 tetrabytes of data. Chinese hackers are downloading intellectual properties estimated at US $ 40-50 billion each year from the US.

China's experimentation with cyber espionage, hacking and

cyber attacks coincided with the advances in its cyber strategy. US cyber security experts first detected penetration attempts by Chinese hackers of US computer networks in 2002. Official US estimates in 2008 noted that Chinese hackers mainly targetted US defence computers and systems and downloaded 10 - 20 tetrabytes of data. Chinese hackers are downloading intellectual properties estimated at US $ 40-50 billion each year from the US. In mid-2009 the US suspected China of shutting down a power plant in the mid-West by a cyber 'attack'. China's hostile cyber activity has attracted international attention because of its dominant military component. US and UK both recently established Cyber Commands and a vigorous debate is underway as to whether a military response, including precision missile strikes, is justified in event of cyber attacks on critical targets. Majority opinion favours such a response.

'Communications Technology', which includes platforms like the internet, mobile and satellite telephone networks, is another potential Achilles' heel for many countries and especially developing nations. In India alone there are an estimated 400 million mobile phone users. Modern communications technologies, which merge mobile and satellite telephones with the internet, heighten the quantum of disruption that could be caused by a hostile 'attack'. The potential for damage was highlighted in a confidential document by the Chairman of Britain's Joint Intelligence Committee, who asserted that equipment installed by the Chinese telecom company, Huawei, in British Telecom's new communications network could be used to halt critical services like power, food and water supplies.

US and UK both recently established Cyber Commands and a vigorous debate is underway as to whether a military response, including precision missile strikes, is justified in event of cyber attacks on critical targets. Majority opinion favours such a response.

The threat is enhanced by the efforts of the PLA to co-opt Chinese telecommunications companies in their cyber warfare programme. In 2003, the Guangzhou Military Region established Information Warfare (IW) militia units and used local telecommunications companies to draw personnel, financial support and infrastructure. In other words, civilian commercial IT expertise was used to augment the PLA's IW capabilities. PLA officers surveyed Guangzhou's Dongshan District, where the IT sector is concentrated, to identify suitable personnel with advanced degrees, major scientific research achievements and computer networking expertise. The Guangzhou Military Region established four 'Militia Information Technology Battalions' in local telecommunications companies. These Battalions combined offensive and defensive Electronic Warfare (EW) units with separate companies assigned to perform computer network operations (CNO) and electronic reconnaissance and deception. The Battalions were tasked to research operational methods for launching attacks, propagating viruses, jamming information channels and disrupting nodes of enemy networks. In 2006, the Academy of Military Sciences (AMS) officially endorsed the establishment of such IW militia and directed the PLA to make their establishment a priority. Garrison level commands were instructed to establish such units with personnel from local commercial IT companies and universities and, where necessary, to relax age and physical fitness criteria. Measures were taken to prevent unintentional disclosure.

The rapid growth of China's telecommunications companies in international markets facilitated enhancement of the PLA's cyber warfare capabilities. Firms like Huawei, ZTE and Venus are leaders in this sector and closely associated with Chinese government security organisations. Chinese IT and telecommunication companies are part of China's military-industrial-espionage conglomerate and reflect the strategy envisaged while drafting the '863 Programme'. A number of the senior management, or founders, of these companies are former employees of the PLA or PLA-run research institutes. China's leadership, which has deftly combined the country's military and economic strengths to achieve strategic goals, has used its hi-tech communications technology sector to further strategic objectives. Huawei and ZTE are two examples of how Chinese hi-tech telecommunications companies work to supplement China's strategic foreign policy goals.

The hi-tech Chinese telecommunications company, Huawei, is a spin-off from a PLA research institute. Its founder CEO is 61-year old Ren Zhengfei, formerly a senior official of a PLA telecommunications research institute. He founded Huawei in 1988 and the company receives national preferences within the system in sales to the PLA. Huawei is an established supplier of specialized telecommunications equipment, training and related technology to the PLA. Along with others such as ZTE and Datang, it received direct funding for R&D on C4ISR systems capabilities. All these firms originated from state research institutes and continue to receive preferential funding and support. Huawei's accounts ledgers are secret and it is reported to have supplied Baghdad with 'illicit' communications just prior to the US invasion. Huawei has partnered with 'Beto', a Russian telecommunications company that is affiliated to the Russian military and was earlier involved in the production of missiles. Since Huawei commenced international marketing operations its expansion has been rapid.

The Zhongxing Telecom, or ZTE, is another PLA-affiliated telecommunications company that is making inroads into markets abroad. It emerged from the No 691 Electronics Factory under the China Aerospace Corporation subordinate to the PLA. Like Huawei, ZTE enjoys national preferences within the system and both companies are among the five that supply routers, switches and computers to the PLA. Founded in 1984, ZTE currently has operations in 33 countries. According to provincial level Communist Party military newspapers, the ZTE Corp. provides certification training and related engineering training to PLA personnel assigned to communications and IW related positions.

Julong and Venus Technologies Inc. are other specialized telecommunications and IT companies with close links to the PLA. They are actively exploring markets in Bangladesh, Pakistan, Vietnam, Cuba, North Korea, Columbia and Russia.

Huawei, ZTE and other Chinese telecommunications companies are trying to expand into the US and European telecommunications markets mainly to upgrade technology. They are simultaneously securing large contracts, often turnkey, for establishing telephone networks in developing countries and where China has long term strategic interests. Huawei and ZTE are maintaining, or setting up, country-wide land-line or mobile telephone networks in the countries surrounding India namely, Afghanistan, Pakistan, Nepal, Bangladesh, Myanmar and Sri Lanka. Huawei and ZTE have both developed major interests in the Indian telecommunications industry despite the obvious implications for the country's security. Huawei has a major software research centre in Bengaluru and claims to have provided 'cutting edge technology to all the telecom operators' in India. ZTE registered a sales volume of US$ 1 billion in India in 2009. It has tied up with the Russian telecom company Sistema, which recently launched operations in India.

Huawei and ZTE are together the 'main service providers' (MSPs) for the majority of Indian mobile telephone networks and in most cases maintain network operations. Mobile telephones are used by virtually all politicians, bureaucrats, armed forces and security officials and industrial tycoons and confidential subjects are routinely discussed. Huawei and ZTE have the access to monitor conversations of persons of interest and selectively disrupt, or terminate, communications. In times of crisis or hostility they could disrupt the country's entire mobile telephone network causing widespread confusion, systems breakdowns, damage and financial and material loss. Other entities vulnerable to attack are those using Chinese computer software and hardware. Selection of the New Delhi Railway Station is indicative that public utilities will be targets for cyber attacks.

India is a potential target for Chinese cyber attacks and these could additionally be launched by Chinese companies from within India. Estimates are that China's cyber force has at least 50,000 trained hackers targeting primarily India and the Dalai Lama's establishment.

India is a potential target for Chinese cyber attacks and these could additionally be launched by Chinese companies from within India. Estimates are that China's cyber force has at least 50,000 trained hackers targeting primarily India and the Dalai Lama's establishment. They are based in the Xinjiang-Uygur Autnomous Region. With India and its armed forces getting increasingly 'wired' and a number of Indian companies going hi-tech and global, enhancing cyber security must be a priority. This has to include indigenisation of critical communications networks along with the capability to trace, disable and counter-attack the source of cyber attacks.

Centre for Air Power Studies

The Centre for Air Power Studies (CAPS) is an independent, non-profit think tank that undertakes and promotes policy related research, study and discussion on defence and military issues, trends, and development in air power and space for civil and military purposes, as also related issues of national security. The Centre is headed by Air Cmde Jasjit Singh, AVSM, VrC, VM (Retd) Centre for Air Power Studies.

P-284, Arjan Path, Subroto Park, New Delhi 110010
Tel: +91 11 25699130/32, Fax: +91 11 25682533

Editor: Ms Shalini Chawla e-mail: shaluchawla@yahoo.com