the pioneer

OPED | Thursday, December 11, 2008 | **Print** | **Close**

Our deadly 'dark visitors'

Claude Arpi

The motives of Chinese hackers usually include commercial and military intelligence gathering and the setting up of sleeper spies in the computer networks ready for future strikes

Have you heard of the 'Dark Visitors'? No, these are not Pakistani *fidayeen* landing on the shores of Mumbai, though they may become the most serious threat to India's national security in the years to come.

Remember the US election. According to reports emanating from the FBI and the US Secret Service, the computer networks of Mr Barack Obama and Mr John McCain were attacked during the presidential campaign. *Newsweek* quoted a FBI agent telling Mr Obama's managers: "A serious amount of files have been loaded off your system."

Though both camps had reported that hackers 'from an undisclosed foreign location' targeted their network during the summer, nobody openly dared to say that China was responsible for the attacks. The objective of the hackers seems to have been to collect documents related to the candidates' future policies.

The recurrence of this type of wild hacking, however, worries many security experts in the West. In December 2007, the US Commerce Secretary Carlos Gutierrez travelled to Beijing to discuss with Chinese officials. The *National Journal Magazine* in an article *China's Cyber-Militia* in May 2008 alleged that Mr Gutierrez was also targeted: "Spyware programmes designed to clandestinely remove information from personal computers and other electronic equipment were discovered on devices used by (the US Secretary)."

According to the US magazine, these spyware programmes are "designed to open communications channels to an outside system, and to download the contents of the infected devices at regular intervals."

When *National Journal* interviewed Rich Mills, the US Commerce Department spokesman, he did not confirm or deny the reports.

The attacks are not confined to the United States. In May, the news came out that Chinese hackers had broken into the computer network of the Indian Ministry of External Affairs (MEA).

As the *Financial Express* put it: "The bad guys are at it again and with increasing ferocity, attacking anything and everything," but this time it was against India.

The motives of Chinese hackers usually include commercial and military intelligence gathering and the setting up of sleeper spies in the computer networks ready for future strikes. An official of the informatics division at the MEA confidently told the *Financial Express*: "They attempted to hack in, but were not successful."

The Government refused to specify who the hackers were, but the IP addresses left behind suggested that the attack originated from China. As the attacks coincided with the unrest in Tibet, many observers believe that the hackers were trying to find out the Tibet policy of the MEA before the Olympic Games. Apparently, the Chinese hackers cracked the security code of a computer network in Beijing and possibly accessed official (encrypted or not) emails in which policy matters may have been discussed.

As usual, New Delhi tried to downplay the incident.

But who are these hackers?

A new book, *The Dark Visitor*by Scott J Henderson answers many of these questions. The author first gives a historic of the hacking business in China with few individuals in the late 90's; he details the emergence of today 'celebrated' (in China at least) groups such as the Honker Union of China and Red Hacker Alliance. He then analyses in detail their methodology, hierarchy, 'who they are', their exploits and the content of their sites (which teach hacking to the public).

Wan Tao, the leader of China Eagle Union hacker group, also known as the 'godfather' of Chinese hackers, explains the distinction between regular hackers and the famed Red Hackers: "Years ago, it was OK to be a hacker, when it simply referred to someone who would break into systems. But over the past decade, the attributes of hackers have become somewhat darker. Chinese hackers coined the word 'Red Hacker', which means someone's a patriotic hacker. Unlike our Western counterparts, Chinese hackers tend to get more involved with politics because most of them are young, passionate and patriotic."

The most fascinating (and frightening) aspects of the Chinese hackers is that they are individuals with only loose links to the Government. Henderson explains, “One of the unique aspects of the Chinese hacker organisation is their nationalism, which is in stark contrast to the loner/anarchist culture many associate with the stereotypical Western hacker. They are especially active during periods of political conflict with other nations.” This sense of patriotism and their own ‘code’ make them act for China’s national honour and never hack inside China.

Two distinct groups are today working in China: One is a civilian ‘independent’ organisation (such as the Red Hacker Alliance) and the other, the official one, the PLA.

When the question is put to Henderson about “tasking, oversight, and control of the organisation”, his answer is simple, “(the hackers) are not a branch of the Government or the military”. They are just an “independent confederation of patriotic youth dedicated to defending China against what it perceives as threats to national pride”.

In his in-depth study, he has not found any evidence of direct Government control. However, the Chinese society does not function with the same parameters as the West (or India). The Chinese Government considers its citizens as “an integral part of Comprehensive National Power and a vital component to national security”.

Can we imagine in India a few lakhs of IT engineers providing regular inputs to the R&AW or the Military Intelligence and undertaking some of its dirty work? Would they attack the US, Chinese or Pakistan networks to get to know the thinking of the leaders of these countries or their plans for forthcoming commercial or diplomatic negotiations?

Is it not invaluable if a party manages to have advanced information on the opposite party’s stand before any negotiations? In India, many will believe that this type of scenario can only be inspired by a Bollywood script, but in China, it is not fiction. It has repeatedly happened to US business persons who as they arrive in China, discover that their Chinese counterparts know everything about their plans.

According to an article, *China’s Electronic Long-Range Reconnaissance* published this month in *Military Review*, Lt Col Timothy Thomas analyses: “Since 2005, Chinese cyber attacks against US systems have increased at an alarming rate.” He, however, adds: “The term ‘attack’ carries unwanted connotations; these unwarranted incursions are more likely reconnaissance missions to collect intelligence… to spot vulnerabilities or plant trap-doors in our systems”.

Interestingly, during the last few years, the PLA’s tactic has undergone a shift from ‘active defence’, (never attacking someone first, but being ready to respond if attacked) to ‘active offence’ which means to undertake “cyber reconnaissance, cyber-stratagem, and computer exploitation activities” before a conflict. Thomas expounds: “IO (Information Operation) tactics and techniques allow more emphasis on the principle of offence than on traditional warfare. A weaker force, for example, can inflict much damage on a superior force with a properly timed and precisely defined asymmetric information attack. China portrays itself regularly as the weaker side of the US-Chinese relationship. It thinks that offensive operations… are key to victory.”

The PLA has no problem using the Chinese war theory ‘attack with a borrowed sword’ which means using thousands of individual hackers who can be co-opted as the need be without the risk of the Government being caught red-handed.

In India, the National Informatics Centre which maintains the Government network says that they are aware of the problem and are taking action to secure the Government systems.

Well, that is ‘active defence’.

During his first visit to Mumbai after taking over as Union Home Minister, Mr P Chidambaram admitted that “there were some lapses in security, coastal or otherwise which need to be rectified.”

But has he even heard of the ‘Dark Visitors’? When it will be too late, a new Minister will probably admit the lapses of his predecessor.