

Cyberwarfare**A Chinese ghost in the machine?**

Apr 2nd 2009 | TALLINN AND TORONTO
From The Economist print edition

Identifying the perpetrator of cyber-attacks can be impossible

CYBERSPACE is ideal for spies. Digitally disguised and undeterred by borders or passports, they can pick locks anywhere in the world, pilfer secrets without trace and even leave toxic traps for the unwary.

Security chiefs are very worried; NATO's new cyberwarfare think-tank in Estonia gets requests for help from across the world. And for researchers outside the charmed circle of high-security clearance, establishing hard evidence of mischief on the net is even harder.

Still, two reports released on March 29th managed to give an intriguing glimpse of the electronic front line, chronicling a systematic surveillance effort, probably controlled by China-based computers, of the Dalai Lama, the Tibetan government-in-exile, and the Tibetan diaspora.

Labelled GhostNet this operation infiltrated 1,295 computers in 103 countries over 22 months, including the foreign ministries of Iran, Indonesia and the Philippines; German, Indian and Pakistani embassies; and organisations such as the Asian Development Bank and NATO.

One report, by two researchers at the University of Cambridge Computer Laboratory in Britain, blamed the Chinese government and drew a firm denial from the authorities in Beijing. The other report, prepared in Canada, was more nuanced. (Both lots of researchers had previously worked in the same research team.)

That China might be using the internet to spy on Tibetan activists' international contacts is less striking, perhaps, than the remarkable ease with which they snooped on victims. Attackers used what are known as Targeted Trojans, e-mails sent to specific individuals that contain malicious software or "malware" hidden in an attached document or photo, or a link to an internet site to which the recipient is directed. To fool the victim, the sender poses as someone the recipient knows.

To make that disguise plausible, the sender must find out the victims' trusted contacts, their style of writing and preferred topics. The case cited in the investigation involved someone posing as a member of the Free Tibet group who sent a translation of a book—to a Tibetan monk.

When the attachment is opened, the malware burrows deep into the computer where it ferrets around for useful information, sends it back to the controlling computer and asks for further instructions.

Targeted Trojans are increasingly popular with spies and criminals. MessageLabs Intelligence, a British firm that monitors security threats, detected one or two per week in 2005, but is now seeing an average of 50 per day, says Paul Woods, the firm's senior strategist. The software does not require the resources of a state intelligence agency; it can easily be found on the internet. This is one reason why the Canadian researchers (at the University of Toronto and SecDev Group, a think-tank) were reluctant to say firmly that China's government mounted the attack on the Tibetans.

Much of the available malware emanates from China, whose 300m internet users represent the largest national group in the world. "We have reached the age of do-it-yourself signals intelligence," concludes the Canadian report.

As amateurs join the professionals, it is hard to tell whether mischief in cyberspace is the work of patriotic hackers, groups of individuals, or a government. The 2007 assault that nearly shut down Estonia's digital infrastructure was blamed on Russian ire over the moving of a Soviet war memorial. But that attack came from a "botnet"—a network of infected machines round the world—including many in America. The sale and rent of botnets is an established criminal business on the internet. An activist with a pro-Kremlin group has said that he mounted the attack on his own initiative. Other recent cyber-attacks have coincided with conflicts between Israel and Hamas, and Russia and Georgia.

Cyberdefence efforts so far have focused on making networks more resilient. Progress on a global legal framework to control internet crime has been minimal, says a NATO cyberwarrior in Tallinn. If a host government refuses to probe further, as is the case with China, little can be done. "You need the right to send someone to the other side of the world with a search warrant to look at someone's computer, when that person may have no idea that it is even infected," says the official.

But it is not only governments which may need to rethink their approach. Software designers could also do more to build security into products so that computers are harder to hijack, says Shishir Nagaraja, an academic at the University of Illinois who studied the Dalai Lama's computers.

Victims of cyber-attacks should perhaps worry less about humiliation and more about helping others to escape the same fate: a novel aspect of the Tibetan episode was that the Dalai Lama and his followers suspected their computers had been infiltrated, called in experts and then allowed the results of the probe to be published. Government and corporate leaders elsewhere might ponder his example.

Meanwhile, the furore is fuelling suspicion of Chinese motives. In Britain Huawei, a Chinese firm, is one of the main contractors in a £10 billion (\$14 billion) effort to upgrade the telephone system. Huawei's boss, Ren Zhengfei, is a former Chinese army officer, and Britain's spies fret that network equipment that will be used by firms, households and government departments could come with hidden "backdoors" that would let Chinese snoopers evade easy detection. In 2008 America's Congress blocked Huawei's plans to buy 3com, another computer-equipment firm, citing similar security worries. Cyberwarfare is a business with a future.