The Economist

Special report:

China and the internet

Cyber-hacking

Masters of the cyber-universe

China's state-sponsored hackers are ubiquitous—and totally unabashed

Apr 6th 2013 | From the print edition

CHINA'S SOPHISTICATED HACKERS may be the terror of the Earth, but in fact most of their attacks are rather workaday. America and Russia have hackers at least as good as China's best, if not better. What distinguishes Chinese cyber-attacks, on anything from governments to *Fortune* 500 companies, defence contractors, newspapers, think-tanks, NGOs, Chinese human-rights groups and dissidents, is their frequency, ubiquity and sheer brazenness. This leads to an unnerving conclusion.

"They don't care if they get caught," says Dmitri Alperovitch, who used to work at McAfee, a computer-security firm, where he helped analyse several Chinese hacking operations in 2010 and 2011, and is a co-founder of CrowdStrike, another cyber-security firm. The indiscriminate tactics of China's 2010-11 campaign made it relatively easy to track. His team identified more than 70 victims (among many more unidentified ones), dating back to 2006, and found that the average time the hackers stayed inside a computer network was almost a year. "They'll go into an organisation and then stay there for five, six years, which of course increases the chances that they get caught."

Mr Alperovitch offers two reasons for the careless abandon of China's hackers. The first is that their attacks are on an industrial scale—"thousands of continuous operations"—so they could hardly be expected to go unnoticed. The second is that "they don't see any downsides to being caught. They have so far not suffered economically or politically for being caught."

It is true that most victims are unwilling to remonstrate openly with the Chinese state. Except for Google, hacked companies have tended to keep quiet. Most governments have chosen not to confront China publicly, though American officials have recently started doing so. NGOs working in China have said nothing. Companies fear reprisals from customers and shareholders for failing to secure their networks. And perversely many victims do not want to antagonise their attackers. Even security companies, though obviously keen to capitalise on the threat, are wary of pointing the finger because they want to sell their antivirus products in China too.

This culture of secrecy and shame makes it harder to confront the problem. It also helps Chinese officials, who consistently and emphatically deny allegations of state-sponsored hacking. They rely on the hope that in such a murky field the evidence is always wanting. Yet in reality it is often fairly plain, and attitudes may at last be hardening. That could mean growing suspicion of the big Chinese technology companies, including Huawei, which is already politically unwelcome in America, and Tencent, which is trying to expand its social-media services abroad. But it is not clear what, in practice, America and other Western countries can do to restrain Chinese behaviour, other than becoming better at hacking themselves.

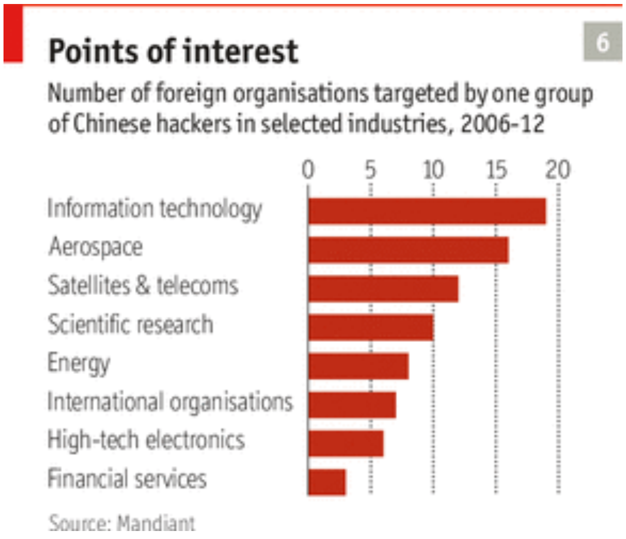
Whodunnit?

Security experts outside China have learned how to reverse-engineer methods of attack and trace attackers' internet-protocol addresses back to their physical origins. They have identified up to 20 “Advanced Persistent Threat” teams operating in China, including one that stole valuable commercial secrets from Google, Adobe and other Silicon Valley companies; another that for years targeted a number of global energy companies; and yet others that have hacked hundreds of companies, government agencies, think-tanks and NGOs the world over. The victims have included global steel companies; a firm that supplies remote-control systems for American oil and gas pipelines and power grids; a hotel computer system that provided access to data for important guests; a tech-security firm, RSA, that opened the way to hacking Lockheed Martin and defence subcontractors producing America's F-35 Joint Strike Fighter; and even NASA. Some of the attacks have been highly sophisticated, but many more have begun with a simple “phishing” e-mail fooling the recipients into clicking on a link.

The organisation and scale of these attacks, involving large teams of hackers and thousands of computers, strongly suggest that the Chinese party-state has played a guiding role. American experts point to the People's Liberation Army's 3rd Department, which according to the Project 2049 Institute, an American think-tank, is roughly equivalent to America's National Security

Agency. Project 2049 describes an apparent fixation with North American targets at the Shanghai headquarters of Unit 61398, part of the 3rd Department. In February Mandiant, a security firm, identified Unit 61398 as the likely base for thousands of attacks on North American corporate and security targets.

The choice of targets also clearly points to China's government as the perpetrator. The Google hack, at a time when the company was facing increasing hostility in China, appeared to leave little room for doubt; one Chinese source actually told officials in America's State Department that two members of the elite Politburo Standing Committee ordered the attack, according to a State Department cable that was released by WikiLeaks. Other victims of hacking attacks included the International Olympic Committee and the World Anti-Doping Agency after the 2008 Beijing Olympics; Tibetan and Uighur activists and Chinese dissidents; think-tanks that analyse China (including its hacking capabilities); and NGOs operating in China. None of these seemed to have any commercial value.



Source: Mandiant

For an individual caught up in such an attack the effect can be creepy. One day in early 2010 an American working for an environmental NGO in China noticed something odd happening on his BlackBerry: it was sending an e-mail from his account without his doing. He watched, dumbfounded, as the e-mail went out to a long list of US government recipients, none of which was in his address book. Seconds later he saw the e-mail disappear from his sent folder. Eventually he heard from the FBI that his e-mail account and those of several colleagues had been compromised by hackers from China. All the victims had attended a climate-change conference in Copenhagen in December 2009 where America and China had clashed.

Another obvious target was David Barboza, a journalist on the *New York Times*. In October 2012 he reported that relatives of Wen Jiabao, then China's prime minister, had amassed assets of $2.7 billion. After the story was published, said the newspaper, Chinese hackers compromised its networks to get at Mr Barboza's work e-mail account. Following the newspaper's disclosure in January, other news organisations, including the *Wall Street Journal* and Reuters, noticed similar Chinese intrusions. But Bloomberg, which last year reported on the finances of relatives of Xi Jinping, China's new president, and has extensively investigated Chinese hacking, has denied suggestions that it was itself successfully hacked.

The Chinese authorities, which since the report on Mr Wen have blocked the *New York Times*'s English and Chinese-language websites, angrily denied the newspaper's hacking allegation. Wan Tao, one of China's first "patriotic hackers" (nationalists who in the early days of China's internet hacked into websites of foreign governments on their own initiative), offers a convenient alternative culprit: "underground hackers", or black-market operators who either sell their services or strike out on their own in hopes of finding a buyer. "Their business model is to sell," Mr Wan says, sitting in front of a ThinkPad in a coffee house in Beijing. The price of access to a target's e-mail box starts at less than $1,000, he says.

But Mr Wan's explanation is unconvincing. His own story offers evidence that what may have started as independent hacking has evolved into a state-supported enterprise. He is now a cloud-security consultant but was an "angry young man" in the 1990s, he says. In 1997 he joined China's first hacking group, "Green Army", leading attacks on foreign websites. His first (solo) patriotic hack, in 1997, was to crash the e-mail box of the Japanese prime minister's website; in 2001, after an American spy plane collided with another plane, he and fellow patriotic or "red" hackers conducted various attacks on American websites in what they quaintly called a "cyberwar".

The quick and the dead

The authorities gave Mr Wan and other hackers free rein. Police did not worry about hacking of targets outside the country, and still do not appear to. China has so far failed to sign an international cybercrime convention. Although hacking has been a criminal offence in China since 1997, the authorities have enforced the law only when the perpetrators were targeting things like state secrets and assets. The first publicised hacking trial in China, in 1998, was of two men who got into the website of a state-owned bank in Jiangsu province, stealing less than $100,000. One of them was executed.

In contrast, patriotic hackers like Mr Wan were sought out for their advice and expertise. In 1998 the cyber-police, then quite newly formed, approached Mr Wan at a security conference in Guangzhou. They wanted him to help them find out who had written anonymous subversive postings on bulletin boards. In response he designed a software system in 1999 that could analyse posts about sensitive subjects such as Falun Gong or democracy, compare them with other online content and find out who had written them. He believes it was the first of its kind in China. "I'm a security expert," he explains. "They had the need."

Later, after his hacks against America, says Mr Wan, he was asked for help by the People's Liberation Army (PLA). He did not want to work for them but agreed to introduce them to other hackers. Since then the PLA has openly recruited hackers, sponsoring contests at universities and posting job advertisements.

The Chinese army's doctrine of cyber-warfare (like that of a number of Western counterparts) is to knock out the enemy's information infrastructure, and its doctrine of cyber-security is to go on the offensive to defend itself against attacks. The Chinese authorities often point out, correctly, that they are the victims of frequent cyber-attacks from America. Thousands of such attacks are also carried out from Russia and Brazil every year. But more of them originate from China than from anywhere else in the world, and at least some of them are undeniably linked to the party-state. That Chinese model may well prove attractive to other countries.

From the print edition: Special report