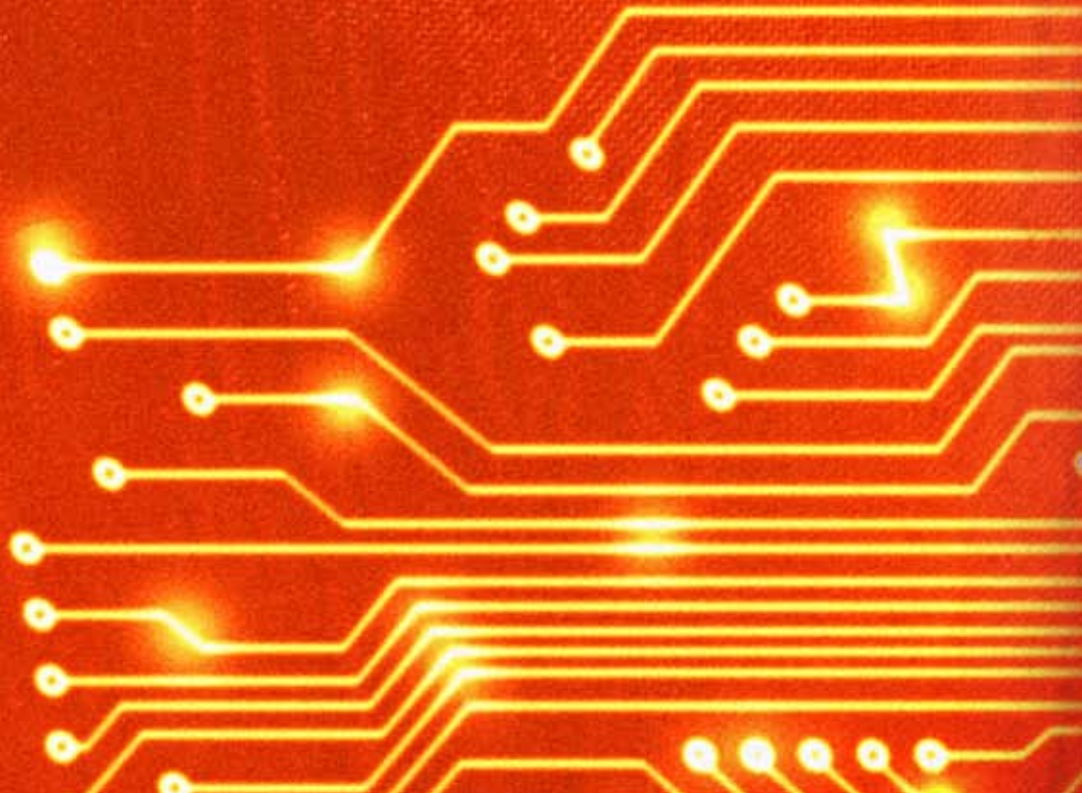




 KCS Country Risk & Threat Advisory

Risk Briefing Paper: China & Cyber Crime
20 December 2011



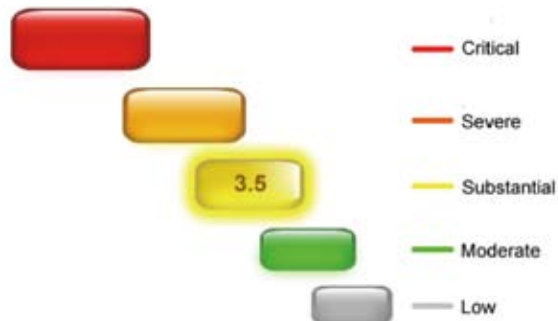
Risk Briefing Paper: China & Cyber Crime



Country: China
Population: 1,338,299,500 (2010 Census)
Source: World Bank, World Development Indicators

China has a Critical risk/threat rating of 3.5

- 5 Critical** Incidents that pose significant risk to the life, health, security and safety to travellers.
- 4 Severe** Incidents that pose significant danger or disruption.
- 3 Substantial** Incidents that pose localised danger.
- 2 Moderate** Incidents that may cause disruption: public demonstrations, airport, airline delays, etc.
- 1 Low** Informational based notification such as a political event, public holiday or public event.



Chinese and Russian state endorsement of cybercrime strongly suspected

In a report addressing cybercrime issued at the start of 2011, KCS advised that the sheer scale of cyber-related-crime originating in countries such as China and Russia had turned the phenomenon into a major international security concern. KCS wrote that businesses would have little choice but to prepare for sophisticated attacks on computerised database systems and internet traffic hijacking looking ahead. As the year winds to close, KCS sees little justification in reviewing its previous outlook. With particular reference to China, there is little room to be complacent.

For much of 2011, Western cybercrime watch-dogs have been advocating a clear and consistent message: that cyber attacks constitute one of the biggest threats to our (essentially economic) security, and that Russia, and even more particularly, China, are the main sources of such threats. Of even greater concern appears to be the fact that Western sources appear convinced that cyber attacks aimed at international economic assets emanating from China, and Russia, may often be sponsored, if not driven, by government departments and state security agencies from these countries.

China cyber threat drawing attention of policy makers at highest level

Earlier this year a report issued by an American government national security office stated that cyber attacks by Chinese and Russian intelligence services, as well corporate hackers in those countries, have swallowed up large amounts of high-tech American research and development data, and that stolen information has helped build their economies. Computer attacks by foreign governments are on the rise and represent a “persistent threat to U.S. economic security”, according to this source. Such threats are only likely to grow further in the short term, as the “the governments of China and Russia will remain aggressive and capable collectors of sensitive U.S. economic information and technologies, particularly in cyberspace.”

Western intelligence agencies feel that China, in particular, has made industrial espionage an integral part of its economic policy, stealing company secrets to help it outdo the U.S. and other foreign competitors to further its goal of becoming the world’s largest economy. Although security experts and officials alike have warned of cyber attacks emanating from China for some time, the US document reflects the growing recognition that the problem is now reaching the undivided attention of government policy makers at the highest level.

Western sources adamant of Chinese economic espionage

While incidents of cybercrime have always been hard to prove due to the difficulty with attributing computer hacking and other types of intrusions into computer systems to any one given source, there

is now sufficient documentation to suggest that foreign spies and organised criminal groups (OCGs) are stealing economic secrets remotely. Cyber crime is at its peak. Westerns sources are adamant that Chinese actors are the most active and persistent perpetrators of economic espionage based on cybercrime-related methods. This year has seen an absolute tidal wave of computer network intrusions that have originated from China and Russia, although the latter ranks a distant second to those when compared to China, according to U.S. government sources.

The aforementioned US government report spoke of up to US\$50 billion being lost (by US business) due to various forms of cyber-crime including espionage, cyber-attacks and other counterfeit and trademark crimes, while referring to sources such as the U.S. International Trade Commission. Information recently released by U.S. intelligence sources suggests that as few as 12 different Chinese groups, allegedly backed or controlled by Chinese government agencies, are responsible for the bulk of China-based cyber attacks stealing critical data from American companies and government departments. KCS has already mentioned the China-based computer-spying network, GhostNet, in previous a writing on China cybercrime. In March 2009, it was revealed that GhostNet had tapped into classified documents from government and private organisations in some 103 countries, including the computers of Tibetan exiles. China has denied these allegations, however.

British companies forced out of business by cyber menace

In October of this year, the head of the UK Ministry of Defence (MOD)'s Cyber Security Program, Major General Jonathan Shaw, went on record to say that targeted cyber attacks by foreign governments and corporations are regularly putting (British) companies out of business. Such attacks are now estimated to cost the British economy £27 billion per year, according to the MOD source. Major General Shaw named China as the main culprit in such attacks, stating that, "the Chinese pose the biggest threat, regularly targeting British companies and government institutions to steal sensitive information." France has likewise been recently targeted in cyber attacks against the French finance ministry by hackers using internet addresses in China, while KCS wrote earlier in the year that Germany detected a sharp rise in cyber attacks during 2010.

Cybercrime now ranks amongst the top four types of global economic crime

The rising tide of cybercrime being witnessed internationally is also duly confirmed by the private sector. While Chinese officials normally reject accusations that their security agencies or military structures are behind cyber attacks against Western economic or state targets, Beijing largely acknowledges the fact that the cybercrime phenomenon is itself growing. China often sees itself as the victim of such attacks, as KCS has highlighted in its last report. However, the fact that last month, the international

consulting firm, PricewaterhouseCoopers (PwC) named cybercrime as one of the top four global forms of economic crime, will not reduce tension levels (between Chinese and Western officialdom in their rhetorical skirmishes about the nature and validity of the cyber threat emanating from China).

No answer to the cybercrime phenomenon from the world's corporates

In a very freshly published annual survey (in November of this year), PwC reported that economic crime hit 34% of companies around the world in the last 12 months, with 10% reporting losses of over US\$5 million. While theft remained the most common form of crime (with 72% of respondents reporting incidents in the past year), almost a quarter of respondents to the survey indicated that they were victims of cybercrime. This is an increase of 13 percent from 2009. The rather stark message from the PwC survey in relation to cybercrime is that companies are at risk from virtually anywhere on the planet where there is a computer, a smart phone or any other device able to access the internet.

No less striking is that the survey confirms that, “no industry or company in any country is immune.” While it is encouraging to note that around half of the respondents in the survey indicated that they were currently more aware of the threat of cybercrime (than in the past), less encouraging was the fact that most did not have (or did not know of) a company plan to effectively address the issue. PwC surveyed close to 4,000 corporate respondents across 78 countries to reach its findings. All indications now point to the fact that the cyber plague is reaching bubonic proportions, with no antidote yet available to either treat the present malaise or to prevent future outbreaks.

Cyber attack victims often fail to grasp full impact of damages

While Western (particularly government) sources tend to point the finger at China as the source of cyber attacks against Western economic targets, companies are often reluctant to reveal the true extent of losses suffered in such attacks for a variety of reasons. Many do not know the extent of the damage themselves, given that corporate victims being targeted in a cyber attack may not even realise that an intrusion has actually taken place, or that their intellectual property or other confidential material has been compromised.

Furthermore, putting a price tag on lost intellectual property is rarely a straightforward task, given the different value that intellectual property may have for the inventor compared to the thief. It is even more difficult to put a price tag on losses resulting from cyber intrusions into computer networks which house information related to national security and other similarly sensitive information. While Western governments tend to be quite bullish in reporting purported cyber attacks, many companies, particularly banks and law firms, are often reluctant to do the same so as not to alienate clients and shareholders

alike, lest to awaken them to the prospect of client confidentiality having been compromised. Quality information about cyber attacks on corporate stakeholders rarely tends to reach the public domain and that which does, tends to be coated by shades of grey. Many questions remain unanswered.

Oil and gas field exploration and bidding contracts an attractive target

Therefore when the computer security firm, McAfee, stated in a report in February 2011 that, “hackers working in China broke into the computer systems of five international oil and gas companies in order to steal bidding plans and other critical proprietary information”, it likewise declined to identify the five companies that had been hacked. McAfee stated that another “seven or so (oil and gas) companies had been hacked” but that the firms could not be identified either.

McAfee aptly dubbed the attacks Night Dragon and released a statement in which it spoke of the “sad state of our critical infrastructure security.” It also said that these were not sophisticated attacks, yet they were successful in achieving their goals: during the last two-to-four years the hackers had access to the computer networks (of the companies) and focused (their attacks) on financial documents related to oil and gas field exploration and bidding contracts. McAfee confirmed that the hack was traced back to China via a server leasing company in Shandong Province that hosted the malware (i.e. malicious software) and to Beijing internet addresses. However, the security firm stopped short of pointing the finger at any specific person or group that may have been behind the attack, stating that there was no evidence “that this was government sponsored in any way.”

Canadian law firms likewise targeted by China hackers

Last month, another report from an international consulting source exposed hackers linked to computers in China engaged in cyber attacks on major Canadian (Bay Street, Toronto) law firms, financial institutions and public-relations agencies. The attacks, in which security specialists believe at least seven leading law firms were targeted, are allegedly linked to an unidentified third party’s effort to seek insider information about a 2010 abortive takeover attempt of Potash Corporation of Saskatchewan (Canada). The consulting source providing information about the hack at the law firms suggested that most of these intrusions were in fact a smokescreen intended to distract attention from the hackers’ real goal: obtaining information about BHP Billiton Ltd’s ultimately unsuccessful US\$38 billion bid for Potash Corporation in 2010.

Sources believe that these rather sophisticated attacks appeared to originate from Chinese computers, bearing in mind that Sinochem Group, China’s state-owned chemicals and fertilizer enterprise, was contemplating an acquisition bid for Potash out of fear that BHP would control the global potash supply.

That being said, and bearing in mind the relentless finger pointing campaign directed at China by Western cyber watchdogs, the source could not confirm whether that attacks were indeed sanctioned by China's government or even whether any sensitive information actually ended up in the hands of hackers.

Hackers force British wind turbine maker out of business

While the two sets of cyber attack case studies highlighted above demonstrate that quality details about the nature of such hacking incidents remain in murky waters, KCS advises that it is fair to assume that companies which may be the proprietors of sensitive information related to China's economic interests could find themselves targeted in similar attacks to those briefly outlined above. In this context, any company bidding on (or assisting with) China related contracts in the energy or natural resources sector, large scale government tenders or procurement projects, or for that matter any other investment project of a large scale, needs to be particularly vigilant.

That being said, given the global reach of the internet, no place and nobody is entirely out of reach. To the contrary, as the MOD's Major General Shaw reminds us: "the moment you come up with a brilliant new idea, it gets nicked by the Chinese and you can end up with your company going bust."

General Shaw's straight talking approach should not be taken out of context. A British firm that had developed a revolutionary design for wind turbine blades in Warrington, Cheshire, was reportedly forced out of business after hackers stole the company's blueprint for the blade and produced a cheaper version (of the blade) overseas.

Attempt to steal information at leading U.S. defence contractor unsuccessful

Such examples of the costly impact of cybercrime are most instructive and carry a strong message for international business. Smaller companies, in particular, need to ensure that they have all possible safeguards in place in order to prevent following in the footsteps of the Warrington-based wind turbine producer. Shortcut solutions and under-investment in appropriate security measures could result in highly damaging consequences. Nothing should be taken for granted. Larger companies tend to be logical targets for the China-based-hacker community, given that the intellectual property data stored on the computer networks of companies such as Google Inc, Intel Corp or Lockheed Martin Corporation can be worth their weight in gold to governments and criminal groups alike.

All three companies have been subject to sophisticated cyber intrusions emanating from China recently. Yet large companies, particularly industrial concerns with close ties to national strategic interests, tend to invest heavily in appropriate cyber defence technologies. Lockheed Martin, the U.S. defence contractor,

reported that the information security breach at RSA, a leading U.S.-based security company, resulted in an ultimately failed attempt to steal sensitive information from Lockheed.

China hacker community targets hundreds of U.S. companies

That being said, cyber security experts are now pointing to the fact that the case of the above mentioned British company is hardly an isolated example (of cybercrime) and that intrusions may target companies of any size and any sector. Earlier this month, analysts revealed an alleged cyber attack by China-based hackers on iBahn, a small, Salt Lake City, Utah-based provider of internet services. iBahn provides broadband business and entertainment access to guests of Marriott International Inc and other hotel chains, including multinational companies that hold meetings on site. Cyber analysts have explained the significance of the attack in that breaking iBahn's networks would potentially allow hackers to see millions of confidential e-mails, even encrypted ones, cashing in on confidential discussions between executives from Dubai to New York (using iBahn's e-networks) on everything from new product development to merger negotiations.

Even more worrisome is the fact that hackers might have used iBahn's system as a launching pad into corporate networks that are connected to it, using travelling employees to create a backdoor to company secrets. Chinese hackers' interest in companies as small as iBahn illustrates the breadth of China's cyber-spying against firms in the U.S. and elsewhere. Analysts familiar with the iBahn case reveal that at least 760 U.S. companies, research universities, internet service providers and government agencies have had their computer networks compromised by China-based cyber spies. The companies, including firms such as Research in Motion Ltd and Boston Scientific Corp, range from some of the largest corporations to niche innovators in sectors such as aerospace, semi-conductors, pharmaceuticals and biotechnology, according to U.S. sources.

Heading towards an 'e-Pearl Harbour'?

While the impact and breadth of China-based hacking into international businesses computer networks is becoming increasingly apparent, cyber security experts have yet to provide a compelling answer, or to build consensus, about how cyber attacks can either be prevented or lessened in likelihood. Although it has been nearly a decade since hackers traced to Guangdong Province, China, carried out a massive cyber espionage campaign dubbed Titan Rain in 2003, which led to the loss of 10-20 terabytes of classified U.S. government information, many uncertainties, as well as many of the old assumptions (of collusive bidding between non-state hackers and state security agencies) continue to prevail. The regularity of cyber attacks appears to have increased alarmingly since that time, however, and there is little convincing evidence that governments are prepared to clamp down on illegal cyber communities in host countries.

To the contrary, the regularity of cyber attacks is rising alarmingly, which itself may be a reflection of the skyrocketing increase in usage of the internet in countries such as China since the year of Titan Rain. It is almost tempting to say that the situation is getting out of hand, which may at least partially explain the frustrations and the bellicose public rhetoric employed by Western cyber watchdogs. Some voices in the U.S. now talk of being on the brink of an 'e-Pearl Harbour', while others suggest that cyber attacks could (and should) be construed as an act of war. Cooler heads call for a new set of 'Rules of Behaviour in Cyberspace' – a code of conduct among the key actors in the cyber environment in the absence of a major international cyber treaty.

Security experts close to the action, however, inform that, "the events of 2011 suggest that the international cyber security landscape is likely to make public and private organisations remain on unsteady footing in the foreseeable future." As has already been suggested, this year's Christmas message with respect to cybercrime is that no one is exempt from hacking and other forms of cyber attack. The cyber-future remains in the balance. Companies will need to take a strategic and yet even more aggressive approach to cyber security during 2012.