ESPIONS ET CYBERESPIONS CHINOIS:
UNE NOUVELLE RÉALITÉ DES AFFAIRES?

CONFÉRENCIER : MICHEL JUNEAU-KATSUYA

Lectures Optionnelles
Optional Readings

CHINA'S SPIES AND CYBERSPIES: A NEW BUSINESS REALITY?

LECTURER: MICHEL JUNEAU-KATSUYA

Thème: Cyber-espionnage en provenance de Chine

Theme: Cyber-Espionage from China

N.B.: Il y a des milliers d'articles et de livres qui couvrent les activités de cyber-espionnage de la Chine. Les articles suivants résument bien la situation. Les préoccupations sont multiples mais tout le monde s'entend sur l'ampleur de la menace. (MJK)

N.B.: There is thousands of news articles and books covering China's cyber-espionage activities. The following summarized well the general situation. Issues are countless but everybody agree on the amplitude of the threat. (MJK)

From: Foreign Policy.com

China's Hacker Army

The myth of a monolithic Chinese cyberwar is starting to be dismantled. A look inside the teeming, chaotic world that exists instead -- and that may be far more dangerous.

BY MARA HVISTENDAHL | MARCH 3, 2010

A flier for a prominent Chinese hacker's presentation on the how-tos and wherefores of hacking, drawing on sources as diverse as Shakespeare, the Diamond Sutra, and … Google. Click through to view FP's exclusive slideshow.

The autobiography of hacker SharpWinner opens on a bunch of young men in a high-rise apartment thick with cigarette smoke, in an unnamed city somewhere in China. Hacking is hard work, and this particular group, one of hundreds spread across the country, has been at it for hours. But the alpha male of the group, a "handsome and bright youth" -- throughout *The Turbulent Times of the Red Hackers*, SharpWinner refers to himself in the third person -- is unflappable. After he completes a backdoor intrusion into a Japanese website, he takes a break to field text messages from female admirers.

It would be easy to dismiss SharpWinner, who has promoted his book on national television, claiming he has a movie deal in the works, as an attention-hungry stuntman. And in fact, the news that Google and dozens of other companies had been hit by a mammoth attack originating in China this past winter evoked the strong arm of the Chinese government -- not SharpWinner's amorphous world of hacker bandits. The Internet giant **said** the decision to go public with information on Operation Aurora, as the hack has been dubbed, "goes to the heart of a much bigger global debate about freedom of speech." The Chinese government's spying on the email accounts of human rights activists, Google intimated, was behind its threat to pull out of China. (It has yet to **make good** on that claim.)

But a **report** released Tuesday by Atlanta security firm Damballa says the Aurora attack looks like work of amateurs working with unsophisticated tools. That revelation, along with a separate **story** in the *Financial Times* that a freelancer wrote the Aurora code, is focusing attention on China's loose web of cowboy hackers. And SharpWinner -- the leader of a **coalition** including anywhere from 50,000 to 100,000 civilian members and, before he disappeared from public view in 2007, a regular participant in international cyberconflicts, including the 2001 hacker war stretching from China to the White House -- is just the beginning.

The Aurora attacks represented an attempt by hackers apparently based in China to steal valuable information from leading U.S. companies. (So far the list of victims includes Adobe Systems and Dow Chemical, in addition to Google.* Over the weekend, a security researcher told *Computerworld* that Aurora might have penetrated **more than 100 firms**.) Investigators are still trying to understand where Aurora came from and what it means, but already some surprising clues have emerged. The *Financial Times* story followed on the heels of a *New York Times* story **reporting** that researchers have traced the attacks back to two Chinese universities, one of which has long been a training ground for freelance or "patriotic" hackers. Among the implications of these reports: The U.S. understanding of Chinese hacking is seriously out of date.

Western media accounts typically overlook freelancers in favor of bluster about the Chinese government. **Some** pair breathy accounts of cyberwar with images dredged up from 1960s People's Liberation Army propaganda, as if to suggest China has some centrally administered cyberbureau housing an army of professional hackers. Others make improbable or unsubstantiated allegations. Two years ago, a *National Journal* **cover story** claimed Chinese hackers were responsible for the 2003 blackout that crippled much of the U.S. Northeast, an event repeated investigations have attributed to domestic negligence.

In fact, the hacking scene in China probably looks more like a few intelligence officers overseeing a jumble of talented -- and sometimes unruly -- patriotic hackers. Since the 1990s, China has had an intelligence program targeting foreign technology, says James A. Lewis, senior fellow for cybersecurity and Internet policy at the Center for Strategic and International Studies. Beyond that, however, things get complicated. "The hacking scene can be chaotic," he says. "There are many actors, some directed by the government and others tolerated by it. These actors can include civilian agencies, companies, and individuals."

To anyone who speaks Chinese, that chaos is obvious. Google the characters for *heike* -- a transliteration of "hacker" that means, literally, "black guest" -- and you'll come up with pages and pages of results. Sites such as www.chinahacker.com, www.cnhacker.com, and www.hackbase.com contain step-by-step instructions, advertisements for how-to seminars -- *become a hacker in a few short weeks!* -- and screen shots of foreign casualties. And yet they are clearly not the work of the central government. Read on (or don't -- the sites are packed with malware and users visit at their own peril) and you'll find threads roiling with bitter infighting, foul-mouthed forum posts, and photos of scantily clad women.

"There are literally hundreds of these sites," says Scott J. Henderson, an intelligence contractor and former U.S. Army linguist who has written a **book** on Chinese hackers. "They all have different agendas and different personnel. It's not as well-coordinated as everyone sitting down in a room and someone saying, 'You, go write this code.' 'You, go write that.'"

Instead, China's hackers spring up organically. Mix together widespread youth nationalism with a highly wired population -- China now boasts the most Internet users in the world, with **384 million people online** -- and out comes patriotic hacking. The self-described "red hackers" are the product of the "the fact that we live in a time when our country is moving toward prosperity," SharpWinner once said, quite accurately. Prosperity also ensures a market for abundant hacker memorabilia: hacker magazines, hacker T-shirts, and tell-all books like his. While traveling through rural China once, I stumbled across bins in a village store filled with Hacker brand candy. (It tastes like saltwater taffy.)

Every August, top hackers convene in Beijing for a **conference** ostensibly about information security but described by one participant as including seminars on common attack techniques. China's hackerati range from flamboyant prima donnas like SharpWinner to **Sunwear**, a slight, pixie-ish twentysomething who marks his website defacements with the innocuous tag line "**just for fun!**", to **Xiao Tian**, the unattainable femme fatale leader of China Girl Security Team. Many of their causes neatly overlap with the interests of the Chinese government. Take one of the events that drove the development of hacker culture in China: the 1999 NATO bombing of the Chinese Embassy in Belgrade. In retaliation, hackers plastered the website of the U.S. Embassy in Beijing with the phrase "Down with the Barbarians!" Or the targeting of email accounts of the Save Darfur Coalition, which **opposes Chinese involvement in Sudan**, in 2008. Or GhostNet, the cyberspying operation originating in China that was revealed last year to have infected 1,295 computers in 103 countries -- including the Dalai Lama's network in Dharamsala, India. The **University of Toronto researchers** who uncovered the attack have not yet pinpointed its architects, but in a **report** on the attack, they noted the operation could easily be the work of patriotic hackers using "do-it-yourself signals intelligence."

But the fact that these hackers' interests overlap with Chinese policy does not mean they are working on behalf of Beijing, and indeed many of their activities suggest no government interference at all. "Governments are not taking over botnets of compromised computers to conduct denial-of-service attacks," says Dorothy Denning, a professor of defense analysis at the Naval Postgraduate School in Monterey, Calif. It helps, however, that Beijing turns a blind eye to their attacks. An unwritten rule holds that freelance hackers are left alone as long as they target foreign sites and companies. Once they go after information inside China, the government cracks down. For a hacker interested in self-preservation, the choice is clear.

Another part of the bargain appears to be remaining open to government requests. If the *Financial Times* report is correct, Operation Aurora was executed with code developed by a thirtysomething freelance Web security consultant working independently, without government prodding. According to the paper's informant, described as a U.S. government researcher, the hacker simply posted a chunk of the code on a hacking forum, where it found its way into Chinese government hands. "He would rather not have uniformed guys looking over his shoulder, but there is no way anyone of his skill level can get away from that kind of thing," the researcher was quoted as saying.

The rest of the story should become clearer in coming months. But another report traces the attacks to servers at Shanghai Jiao Tong University's **School of Information Security Engineering,** one of China's top computer science schools and a hotbed for freelance hackers. For years, students there have freely organized hacker groups and traded war stories in forums

hosted on the school website. In 2007, Shanghai Jiaotong graduate student and veteran hacker Peng Yinan hosted an information session titled "Hacker in a Nutshell" in a school conference room. The **PowerPoint slides** he worked off -- which until recently could be downloaded from his group's website, now down -- glorify hacker culture and explain successful techniques that can be tried at home, pointing out that *Chicago Tribune* reporters once uncovered contact information for thousands of CIA agents using a basic online service. A **flier** advertising the event described Peng as a consultant for the Shanghai Public Security Bureau.

Another student whose screen name appears on Peng's hacks -- but who told me he wasn't involved -- went on to work for Google.

Could Operation Aurora have been written by a freelancer, picked up by a bureaucrat, and then reassigned to a freelancer with ties to Google? It is a possibility worth entertaining, at least. Some have argued that the Chinese government should have more effective means for securing intelligence than students and online misfits. But others say a decentralized approach suits Beijing just fine. "You can see the benefits of having a blurry line," says Lewis. "The Russians do it all the time with Estonia: 'Of course it wasn't us. Can you prove it was us?'"

Ultimately, a loose connection between Beijing intelligence operatives and patriotic hackers is more troubling than a strong one. Governments operate under constraints. Gangs of young men -- as the United States has learned the hard way -- don't. "Certainly if it's government-sponsored cyberwarfare, I have someone I can deter," says Henderson. "If it's mutually assured online destruction -- OK, I can at least develop a theory on that. But with rogue Internet actors it's very difficult. They're potentially very dangerous."

The thought would flatter SharpWinner. In his TV appearance, he confided his concerns about hacking culture in China. He had witnessed the disintegration of some prominent hacker groups, and he fretted that most patriots simply get on board whenever some international incident flares up and lay off hacking foreign companies once things cool down. But with a little effort these challenges can be overcome, he concluded, saying that he is encouraged by a recent resurgence of interest in hacking. Then he addressed listeners directly. "Brothers," he intoned, "go with me! The future of red hacking is bright!"

**The original version of this article cited reports that RAND Corporation had been hit by Aurora. A RAND spokesman wrote in to say "RAND has not been hit -- we have no evidence of attacks or having been targeted by Aurora."*

http://www.foreignpolicy.com/articles/2010/03/03/china_s_hacker_army

---

from: AP

Hackers 'hiding behind Great Firewall'

Thursday, 4 February 2010

Google's accusation that its email accounts were hacked from China landed like a bombshell because it cast light on a problem that few companies will discuss: the pervasive threat from

China-based cyberattacks.

The hacking that angered Google and hit dozens of other businesses adds to growing concern that China is a centre for a global explosion of internet crimes, part of a rash of attacks aimed at a wide array of targets, from a British military contractor to banks and chemical companies to a California software maker.

The government denies it is involved. But experts say the highly skilled attacks suggest the military, which is a leader in cyberwarfare research, or other government agencies might be breaking into computers to steal technology and trade secrets to help state companies.

"Chinese hacking activity is significant in quantity and quality," said Sami Saydjari, president of the consulting firm Cyber Defence Agency and a former US National Security Agency official.

Officials in the United States, Germany and Britain say hackers linked to China's military have broken into government and defence systems.

But attacks on commercial systems receive less attention because victims rarely come forward, possibly for fear it might erode trust in their businesses.

Google was the exception when it announced 12 January that attacks hit it and at least 20 other companies. Google says it has "conclusive evidence" the attacks came from China but declined to say whether the government was involved.

Google cited the attacks and attempts to snoop on dissidents in announcing that it would stop censoring results on its China-based search engine and leave the country if the government does not loosen restrictions.

Only two other companies have disclosed they were targets in that attack - software maker Adobe Systems and Rackspace, a Web hosting service.

Mikko Hypponen, chief research officer at Finnish security software maker F-Secure Corp., said his company has detected about two dozen attacks originating from China each month since 2005.

"There must be much more that go completely undetected," he said.

Hypponen said a large British military contractor with which his company worked discovered last year that information had leaked for 18 months from one of its computers to an internet address in the Chinese territory of Hong Kong. He said similar attacks on military contractors were found in Germany, the Netherlands, Sweden and Finland.

Saydjari said other researchers have told him of dozens of US companies that have been attacked from China but said he could not disclose their names or other details.

A key source of the skills required might be China's military. China's army supports hacker hobby clubs with as many as 100,000 members to develop a pool of possible recruits, according to Saydjari.

"China has a strategic goal of becoming the world-dominant economic power within this century. Certainly one way to do that faster is to steal industrial secrets," he said.

There are no estimates of losses attributable to hacking traced to China, but antivirus supplier McAfee says intellectual property worth an estimated $1 trillion was stolen worldwide through the internet in 2008.

Separately, a Los Angeles law firm says it was hit 11 January by an attack that appeared to originate in China after it filed a lawsuit for CyberSitter, a software maker that accuses the

Chinese government of stealing its code for use in a web-filtering system.

The firm Gipson Hoffman & Pancione said emails sent to its lawyers contained malicious software designed to extract information from their computers.

Security firm Mandiant has dubbed such attacks - which allow repeated thefts over months or years - an "advanced persistent threat" and says each one it has studied over the past five years involved theft of information related to U.S.-China corporate acquisitions, negotiations or military acquisitions.

"The scale, operation and logistics of conducting these attacks - against the government, commercial and private sectors - indicates that they're state-sponsored," the company said in a report last month.

But even if an attack is traced to China, experts need to examine the computer used to be sure it was not hijacked by an attacker elsewhere.

Consultants say security for many Chinese computers is so poor that they are vulnerable to being taken over and used to hide the source of attacks from elsewhere.

In the Google case, confirming the source would require China's cooperation, and Beijing has yet to respond to US Secretary of State Hillary Rodham Clinton's appeal for an investigation.

"The 'smoking gun' proof is very hard to put together," said Graham Cluley, a researcher for Sophos, a British security software company.

China's Industry Ministry said in a statement that any suggestion the government is involved in any internet attack "is groundless and aims to discredit China."

But China is no stranger to government-directed industrial espionage on a vast scale.

Intelligence experts say that since the 1970s, Beijing has carried on a quiet campaign to acquire foreign technology and other secrets by using Chinese businesspeople, students and scientists who travel abroad as part-time spies.

China, with the world's biggest population of Web users at more than 384 million, also has a history of hacking. In 1999, Web surfers defaced US government sites after the mistaken American bombing of Beijing's Belgrade embassy killed three Chinese.

Nationalists have attacked websites in Japan and Taiwan, the self-ruled island claimed by Beijing as its own territory.

More recent cases have shifted from vandalism to theft of government or trade secrets.

Last March, a Canadian group, the Information Warfare Monitor, said it found a China-based ring stole sensitive information from thousands of computers worldwide. Targets included the communications network of The Associated Press.

The government did not respond to the report's details but said it opposes computer crime and criticized the researchers for suggesting otherwise.

China has also ordered vendors that sell computer security technology to government agencies to reveal how it works under rules that take effect on 1 May. Foreign companies operating there worry that might compromise systems used by banks and others to protect customer information and trade secrets.

Beijing is also pressing foreign financial firms to move more of their computer servers into China. That might require a switch to Chinese-made equipment with weaker protections.

Companies' reluctance to talk about China-based hacking "makes it difficult to make the case for action broadly," Saydjari said. "That might be why Google is parting from that history and sounding the alarm."

http://lifeandstyle.independentminds.livejournal.com/1242508.html

---

From The Times
March 8, 2010

Cyberwar declared as China hunts for the West's intelligence secrets

It is estimated that in the past year the number of attacks on US government agencies rose to 1.6 billion per month. Systems in the EU are even more vulnerable

Michael Evans, Giles Whittell

Urgent warnings have been circulated throughout Nato and the European Union for secret intelligence material to be protected from a recent surge in cyberwar attacks originating in China.

The attacks have also hit government and military institutions in the United States, where analysts said that the West had no effective response and that EU systems were especially vulnerable because most cyber security efforts were left to member states.

Nato diplomatic sources told *The Times*: "Everyone has been made aware that the Chinese have become very active with cyber-attacks and we're now getting regular warnings from the office for internal security." The sources said that the number of attacks had increased significantly over the past 12 months, with China among the most active players.

In the US, an official report released on Friday said the number of attacks on Congress and other government agencies had risen exponentially in the past year to an estimated 1.6 billion every month.

The Chinese cyber-penetration of key offices in both Nato and the EU has led to restrictions in the normal flow of intelligence because there are concerns that secret intelligence reports might be vulnerable.

Sources at the Office for Cyber Security at the Cabinet Office in London, set up last year, said there were two forms of attack: those focusing on disrupting computer systems and others involving "fishing trips" for sensitive information. A special team has been set up at GCHQ, the government communications headquarters in Gloucestershire, to counter the growing cyber-threat affecting intelligence material. The team becomes operational this month.

British and American cyber defences are among the most sophisticated in the world, but "the EU is less competent", James Lewis, of the Centre for Strategic and International Studies, said. "The porousness of the European institutions makes them a good target for penetration. They are of interest to the Chinese on issues from arms sales and nuclear non-proliferation to Tibet and energy."

The lack of routine intelligencesharing between the US and the EU also contributes to the vulnerability of European systems, another analyst said. “Because of Britain’s intelligence-sharing relationship with America our systems have to be up to their standards in a way that some of the European systems don’t,” he explained.

Jonathan Evans, Director-General of MI5, warned in 2007 that several states were actively involved in large-scale cyber-attacks. Although he did not specify which states were involved, security officials have indicated that China now poses the gravest threat. Beijing has denied making such attacks.

Robert Mueller, FBI Director, has warned that, in addition to the danger of foreign states making cyber-attacks, al-Qaeda could in the future pose a similar threat. In a speech to a security conference last week, Mr Mueller said terrorist groups had used the internet to recruit members and to plan attacks, but added: “Terrorists have \ shown a clear interest in pursuing hacking skills and they will either train their own recruits or hire outsiders with an eye towards combining physical attacks with cyber-attacks.”

He said that a cyber-attack could have the same impact as a “well-placed bomb”. Mr Mueller also accused “nation-state hackers” of seeking out US technology, intelligence, intellectual property and even military weapons and strategies.To help to fight the growing threat, the Office of Cyber Security, set up last year as part of the Government’s national security strategy, liaises with America’s so-called cyber czar, Howard Schmidt, who was appointed by President Obama to protect sensitive government computers.

British officials said that everyone in sensitive jobs had been warned to be especially cautious about disseminating intelligence and other classified information. Whether British intelligence is involved in retaliatory attacks is never confirmed. However, officials said that there was a significant difference between being part of an information war and indulging in aggressive attacks to disrupt another country’s computer systems.

Dr Lewis said that neither the US nor any of its Western allies had formed an effective response to the Chinese threat, which has its origins in a massive boost to Chinese technology ordered by Deng Xiaoping, the late Chinese leader, in 1986. The West’s own cyber offensives have so far been directed largely at terrorists rather than nation states, giving China virtually free rein to penetrate Western systems with its own world-class hackers and increasingly popular Chinese-made components. “You almost have to admire them,” Dr Lewis said. “They have been very consistent in their goals.”

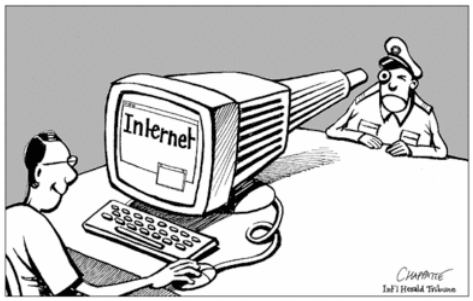
http://technology.timesonline.co.uk/tol/news/tech_and_web/article7053254.ece

Thème: Contrôle et censure de l'internet

Theme: Control and Censorship of the Internet

N.B.: L'existence des « hackers patriotiques » est très important pour le gouvernement chinois. S'il n'y a pas de collusion ou de complicité entre les hackers et le gouvernement chinois, comment peuvent-ils passer la surveillance serrée des contrôles établis sur l'internet? (MJK)

N.B.: The existence of the "Patriotic Hackers" is very important for the Chinese Government. If there is no collusion or complicity between the Chinese hackers and the government, how can they pass around the tight control established on the Internet? (MJK)



From: The New York Time
April 7, 2010

China's Censors Tackle and Trip Over the Internet

By MICHAEL WINES, SHARON LAFRANIERE and JONATHAN ANSFIELD

*This article was reported by **Michael Wines**, **Sharon LaFraniere** and **Jonathan Ansfield** and written by Mr. Wines.*

BEIJING — Type the Chinese characters for "carrot" into Google's search engine here in mainland China, and you will be rewarded not with a list of Internet links, but a blank screen.

Don't blame Google, however. The fault lies with China's censors — who are increasingly a model for countries around the world that want to control an unrestricted Internet.

Since late March, when Google moved its search operations out of mainland China to Hong Kong, each response to a Chinese citizen's search request has been met at the border by government computers, programmed to censor any forbidden information Google might turn up.

"Carrot" — in Mandarin, huluobo — may seem innocuous enough. But it contains the same Chinese character as the surname of President Hu Jintao. And the computers, long programmed to intercept Chinese-language searches on the nation's leaders, substitute an error message for the search result before it can sneak onto a mainland computer.

This is China's censorship machine, part George Orwell, part Rube Goldberg: an information sieve of staggering breadth and fineness, yet full of holes; run by banks of advanced computers, but also by thousands of Communist Party drudges; highly sophisticated in some ways, remarkably crude in others.

The one constant is its growing importance. Censorship used to be the sleepy province of the Communist Party's central propaganda department, whose main task was to tell editors what and what not to print or broadcast. In the new networked China, censorship is a major growth industry, overseen — and fought over — by no fewer than 14 government ministries.

"Press control has really moved to the center of the agenda," said David Bandurski, an analyst at the China Media Project of the University of Hong Kong. "The Internet is the decisive factor there. It's the medium that is changing the game in press control, and the party leaders know this."

Today, China censors everything from the traditional print press to domestic and foreign Internet sites; from cellphone text messages to social networking services; from online chat rooms to blogs, films and e-mail. It even censors online games.

That's not all. Not content merely to block dissonant views, the government increasingly employs agents to peddle its views online, in the guise of impartial bloggers and chat-room denizens. And increasingly, it is backing state-friendly clones of Twitter, Facebook and YouTube, all Western sites that have been blocked here for roughly a year.

The government's strategy, according to Mr. Bandurski and others, is not just to block unflattering messages, but to overwhelm them with its own positive spin and rebuttals.

The government makes no apologies for what it calls "guiding public opinion." Regulation is crucial, it says, to keep China from sliding into chaos and to preserve the party's monopoly on power.

"Whether we can cope with the Internet is a matter that affects the development of socialist culture, the security of information, and the stability of the state," President Hu said in 2007.

In China's view, events since then — including the online spread of the democracy manifesto known as Charter 08 and riots in the Tibet and Xinjiang regions, said to be aided by cellphone and Internet communications — have only reinforced that stance.

In the last year, censorship has increased markedly, as evidenced by the closing of thousands of blogs and Web sites in ostensible anti-pornography campaigns, and the jailing of prominent dissidents who used the Internet to spread their views. The departure of Google's search engine in March only capped months of growing intolerance of unfettered speech.

The paradox — at least at first glance — is that even with such pervasive restraints, China's press and Internet are capable of freewheeling discourse and social criticism.

Newspapers, blogs and online chats have unleashed national outrages over a host of topics, including food and medicine contamination and local corruption. Bloggers continually tweak the censors, leaking their orders and creating an online land of mythical creatures whose names are all homonyms for aspects of the state's heavy hand.

Some exposés and satires fall on the acceptable side of an often invisible and shifting line that

marks what can and cannot be said freely in China. On the other side are statements that too overtly challenge the Communist Party's hold on power, that attack or embarrass powerful politicians or that tread on a long list of forbidden topics, from unrest in Tibet to political crises like the 1989 Tiananmen Square protests.

Journalists and Internet publishers often discover that they have crossed the line only after their online presence is blocked, their bylines are blacklisted or they are detained or summoned to "tea" with government security officers who deliver coy but unmistakable warnings.

With 384 million users in China at last count in January — and 181 million blogs — the Internet poses a true cat-herding predicament for censors. Foreign entities that operate outside China are the lesser of the censors' problems. The reason is logistical: access to the Internet in China from the outside world is limited, and all traffic must pass through one of three large computer centers in Beijing, Shanghai and Guangzhou.

At those centers, government computers — the so-called Great Firewall — intercept inbound data and compare it with a constantly changing list of forbidden keywords and Web addresses.

When a match occurs, the computers can block the incoming data in several ways, from rejecting it outright to making more nuanced trims. For example, Chinese citizens who search Google using sensitive terms like "Tiananmen" may receive complete summaries of relevant Web sites. But if the Web sites are banned, it is impossible to link to them.

Within China, however, data cannot be choked off at a handful of gateways. So the government employs a toolbox of controls, including persuasion, co-opting and force, to keep the Web in line. Self-censorship is the first line of filtering and an obligation of all network and site operators in China.

China's big homegrown sites, like Baidu, Sina.com and Sohu, employ throngs of so-called Web administrators to screen their search engines, chat rooms, blogs and other content for material that flouts propaganda directives. For four years, Google followed suit with its Chinese search engine, Google.cn.

The Internet companies' employees are constantly guessing what is allowed and what will prompt a phone call from government censors. One tactic is to strictly censor risky content at first, then gradually expand access to it week by week, hoping not to trip the censorship wire.

The monitors sit astride a vast and expanding state apparatus that extends to the most remote Chinese town. "There is an Internet monitoring and surveillance unit in every city, wherever you have an Internet connection," said Xiao Qiang, an analyst of China's censorship system, at the University of California, Berkeley. "Through that system, they get to every major Web site with content."

Under a 2005 State Council regulation, personal blogs, computer bulletin boards and even cellphone text messages are deemed part of the news media, subject to sweeping restrictions on their content.

In practice, many of those restrictions are spottily applied. But reminders that someone is watching are pointed and regular.

An inopportune post to a computer chat forum may produce a rejection message chiding the author for "inappropriate content," and the link to the post may be deleted. Forbidden text

messages may be delivered to cellphones as blank screens.

Even so, screening the electronic activities of hundreds of millions of people is a nearly impossible task. Moreover, users increasingly are resorting to technological maneuvers like virtual private networks and proxy servers to sidestep the censors' blocking of banned Web sites altogether. By some reports, a million people now hurdle the Great Firewall via such dodges — a number that remains a tiny fraction of all users, but that has spiked upward in the last year.

So the censors have taken other tacks to tighten their grip.

One is automation. China's leading instant-messaging service, called QQ, automatically installs a program on users' computers that monitors their communications and blocks censored text.

The Ministry of Industry and Information Technology tried last year to expand automated censorship nationwide through mandatory Green Dam software that could remotely update lists of banned topics. After an outcry from Internet users and corporations, the state backed off, but Green Dam or other filtering software remains installed on computers in some Internet cafes and schools. Last month, the government signaled that a version for cellphones was in the works.

Another strategy is manipulation. In recent years, local and provincial officials have hired armies of low-paid commentators to monitor blogs and chat rooms for sensitive issues, then spin online comment in the government's favor.

Mr. Xiao of Berkeley cites one example: Jiaozuo, a city southwest of Beijing, deployed 35 Internet commentators and 120 police officers to defuse online attacks on the local police after a traffic dispute. By flooding chat rooms with pro-police comments, the team turned the tone of online comment from negative to positive in just 20 minutes.

According to one official newspaper editor who refused to be named, propaganda authorities now calculate that confronted with a public controversy, local officials have a window of about two hours to block information and flood the Web with their own line before the reaction of citizens is beyond control.

Zhang Shihe, a self-identified citizen journalist and blogger with the pen name Tiger Temple, said the government ranked various bloggers by the risk they posed. "The most dangerous ones will be shut down, and some others will receive alerts from the government," he said.

Mr. Zhang's own blog posts are sometimes deleted. His workaround is to publish six blogs, hosted on different Internet sites: because censorship rules are vague and the censors merely human, a post that one blocks may be ignored or overlooked by another.

That may not last long. The consensus is that the government is rapidly getting better at its work.

Consider: One chilling new regulation limits those who can operate a site on China's .cn domain to registered businesses, and requires operators to produce Chinese identification. "In case they need to shut you down for some subversive content, they need to know how to find you," said an executive with one Beijing firm that hosts Web sites.

Major cities like Beijing — which last year advertised for 10,000 voluntary Internet monitors — are increasingly taking censorship into their own hands.

Pitted against this are those who argue that government chokeholds on the Internet cannot succeed. Bloggers like Mr. Zhang argue that growing restrictions on Internet speech only inflame ordinary users, and that bit by bit “people are pushing the wall back.”

Or at least trying. At a recent meeting of Chinese Internet leaders in the southern city of Shenzhen, Ding Jian, who heads the Internet company AsiaInfo, proposed that Shenzhen be made a censorship-free zone as an experiment to determine whether China can stomach the chaos of an unfettered Internet. Strangling free speech, one entrepreneur argued, is likely to strangle innovation as well.

The Internet portal NetEase published a report of the meeting. It was quickly deleted.

http://www.nytimes.com/2010/04/08/world/asia/08censor.html

INTERNET POLICE: Meet JingJing and Chacha, the friendly faces of Chinese state censorship who pop up regularly to remind people of the rules.

De: Reporters Sans Frontières
4 décembre 2009

Deux internautes tibétains condamnés à trois ans de prison

Les internautes tibétains **Gyaltsing** et **Nyima Wangchuk** ont été condamnés à trois ans de prison ferme pour "communication d’informations à des contacts à l’extérieur de la Chine", notamment pour avoir téléchargé des photos du dalai lama. La date de leur condamnation n’est pas connue de manière exacte, mais elle remonterait à début décembre.
Ils sont détenus à Lhassa depuis le 1er octobre 2009. Leurs familles n’ont jamais pu leur rendre visite en prison, n’ont reçu aucune information les concernant et s’inquiètent de leur état de santé.

Yeshi Namkha, **Anne** (pseudo) et **Thupten** sont trois autres internautes arrêtés le 1er décembre pour les mêmes motifs. Ils sont toujours détenus, mais n’ont pas encore été condamnés. Le lieu de leur détention est toujours inconnu.

"Ces jeunes internautes tibétains n’ont rien fait de mal en s’échangeant tout simplement des photos du leader spirituel tibétain. Nous demandons leur libération immédiate et l’abandon de

toutes les poursuites à leur encontre. Ces condamnations sont aberrantes : ces jeunes internautes ne doivent pas faire les frais des tensions entre les autorités chinoises et le dalai lama", a déclaré l'organisation.

22.10.2009 - Nouvelles arrestations d'internautes au Tibet
Trois jeunes Tibétains ont été arrêtés 1er octobre 2009 par la police dans le comté de Sogdzong. **Gyaltsing**, 25 ans, **Nyima Wangchuk**, 24 ans et **Yeshi Namkha**, 25 ans, tous les trois résidents du village de Dara, ont été emmenés dans le comté de Nagchu. La police refuse que leurs familles les contactent.

Les autorités chinoises accusent ces jeunes gens de fournir des informations sur le Tibet à des contacts à l'extérieur de la Chine.

"Internet au Tibet est surveillé, censuré et manipulé bien plus que dans les autres provinces de la Chine. Les internautes tibétains, malgré les risques, continuent de faire circuler certaines informations, notamment vers la diaspora et les organisations de droits de l'homme. Il est déplorable que la police chinoise mette autant d'énergie à identifier et arrêter de simples internautes. Nous appelons à leur libération", a déclaré Reporters sans frontières.

Les trois jeunes internautes auraient échangé sur *QQ*, une messagerie instantanée chinoise, des photos et des discours du dalaï-lama. Leurs activités en ligne étaient surveillées, semble-t-il, depuis longtemps par la sécurité publique. Les populations du comté de Sogdzong ont témoigné d'un harcèlement policier, notamment de nombreuses vérifications d'identités.

Des policiers ont ainsi interdit aux moines du monastère Sog Tsandan de célébrer la fin de leur retraite estivale (durant laquelle les moines s'isolent dans le monastère pour ne pas blesser les insectes émergeant durant cette saison), les forçant à assister à des séances patriotiques avec les autorités chinoises.

Reporters sans frontières rappelle que plusieurs internautes et blogueurs ont été arrêtés par la police au cours des derniers mois. Le 12 août 2009, **Pasang Norbu** a été arrêté à Lhassa pour avoir regardé en ligne des photos du drapeau tibétain et du dalaï-lama. **Gonpo Tserang**, guide, a été condamné en juin 2009 à trois ans de prison pour avoir "incitation au séparatisme" et "communications à l'extérieur du pays", après avoir envoyé des emails et des Sms sur les manifestations de mars 2008.

http://fr.rsf.org/chine-deux-internautes-tibetains-04-12-2009,34807.html

---

De: Reporters Sans Frontières
31 mars 2010

Dans l'ère "post-google.cn", la censure et les attaques en ligne continuent, Yahoo ! sommée de s'expliquer

Reporters sans frontières exprime son inquiétude devant les cas répétés de censure et de cyber-attaques sur la Toile chinoise. Les boîtes e-mails *Yahoo !* de plusieurs journalistes étrangers basés en Chine ont fait l'objet de cyber-attaques ces dernières semaines. La version chinoise du moteur de recherche *Google*, basée depuis le 22 mars à Hong Kong, a subi une censure intermittente ces derniers jours. La situation serait retournée à la normale depuis le 31 mars 2010 au matin.

« Nous demandons à *Yahoo !* de faire preuve de transparence et de communiquer sur la nature et l'étendue de ces cyber-attaques. Il est essentiel que ses clients soient informés de la situation, sans quoi *Yahoo !* pourrait sembler couvrir les auteurs de ces attaques. S'agit-il d'attaques généralisées contre les serveurs e-mails *Yahoo !* basés en Chine, ou bien plus ciblées, visant les défenseurs des droits de l'homme et les journalistes, comme celles qui avaient touché *Google* fin 2009 ? Depuis combien de temps durent-elles ? », a demandé l'organisation. « Les autorités chinoises doivent s'expliquer sur la manière dont elles combattent ce genre de cyber-attaques, totalement contraires aux lois chinoises. Il s'agit aussi d'une affaire de cybersécurité. »

Reporters sans frontières suit de près la censure intermittente qui a touché google.com.hk ces derniers jours. « Il est encore trop tôt pour dire si le blocage de la version chinoise de *Google* était volontaire ou le résultat d'une erreur technique, s'il peut être considéré ou non comme un avertissement lancé au géant de l'Internet par les autorités chinoises et si ces dernières préparent le terrain pour la mise en place d'un blocage du site. Cette dernière option constituerait un acte de censure dommageable à la liberté d'expression. »

Le 30 mars, de nombreuses requêtes sur google.com.hk ne donnaient pas de résutats, contrairement à des requêtes similaires sur *Baidu*. Une page d'erreur s'affichait pour des recherches aussi classiques que « China » par exemple. Ce phénomène a été observé principalement dans la région de Pékin, alors que Shanghai semblait moins touchée. *Google* a d'abord expliqué ce phénomène par des ajustements techniques en interne. Le code concerné, décrivant les paramètres de recherche, aurait contenu les trois lettres rfa, un terme bloqué par la « Grande Muraille éléctronique » chinoise, car lié à la radio d'information américaine *Radio Free Asia* (RFA), dont le site est inaccessible en Chine. Des explications finalement remises en cause au profit de la thèse d'un blocage du site par les autorités. L'accès aux services fournis par *Google* en téléphonie mobile serait également partiellement bloqué depuis le 28 mars.

Le 22 mars dernier, *Google* a lancé une version chinoise non censurée de son moteur de recherche en chinois www.google.com.hk. Depuis, à l'exception des blocages de ces derniers jours, des liens traitant de sujets jugés sensibles s'affichent, mais l'accès aux pages concernées est bloqué par le Great Firewall en Chine.

Les censeurs sont très mobilisés autour de « l'affaire *Google* ». Le Bureau de l'Information du Conseil d'Etat a publié des directives limitant la couverture de la décision de *Google* de fermer Google.cn et de ne plus s'autocensurer. D'après des documents obtenus par l'organisation Chinese Human Rights Defenders (CHRD), le 28 mars dernier, les directeurs de sites ont reçu les consignes d'« utiliser seulement les articles des médias officiels », de « ne pas mener d'enquête sur le sujet », mais aussi celles d' « interdire les discussions sur le sujet de *Google* » et de « ne pas reprendre les communiqués et informations provenant de *Google* ».

Les cyber-attaques, qui avaient incité *Google* à fermer Google.cn, n'ont pas cessé. D'après le Foreign Correspondents' Club of China (FCCC), les boîtes e-mails *Yahoo !* d'au moins dix journalistes étrangers basés en Chine et à Taïwan ont été attaquées ces dernières semaines. Le FCCC a reproché à *Yahoo !* de ne pas avoir répondu à ses questions et de ne pas avoir expliqué aux usagers concernés ce qui s'était passé. Des accusations relayées par Clifford Coonan, journaliste pour *The Irish Times*. Il explique qu'un message d'erreur s'affichait lorsqu'il tentait de se connecter à son compte e-mail. *Yahoo !* a déclaré s'être « engagé à protéger la sécurité et la vie privée de ses usagers ».

Kathleen McLaughlin, une journaliste américaine basée à Pékin, a été victime d'une telle attaque. Elle a déclaré à Reporters sans frontières aujourd'hui, « En entrant mes identifiants *Yahoo !* le 25 mars, j'ai reçu un message m'informant que mon compte avait des problèmes et que je devais contacter *Yahoo !* par téléphone pour des questions de sécurité. Au bout de six jours de tentatives infructeuses, l'accès à mon compte a finalement été restauré ce matin. *Yahoo !* ne m'a toujours pas expliqué qui avait accédé à mon compte ni comment ils avaient été informés de ces attaques et quelles informations ont pu être révélées ».

Des cyber-attaques similaires à celles portées contre *Google* ont été identifiées au Viêt-nam. Un logiciel malfaisant aurait infecté des dizaines de milliers d'internautes alors qu'ils pensaient télécharger de simples logiciels. D'après *Google*, ce malware aurait permis d'espionner les utilisateurs touchés et de lancer des attaques de types DDoS contre des blogs contenant des contenus politiques. Ces attaques auraient visé en particulier les sites critiquant l'exploitation par une entreprise chinoise des mines de bauxite au Viêt-nam. Un sujet très sensible dans le pays. L'entreprise de sécurité informatique McAfee Inc, qui a détecté le malware/logiciel malfaisant, a même émis l'hypothèse selon laquelle « ses créateurs ont peut-être des liens avec le gouvernement viêtnamien ».

Par ailleurs, le 30 mars 2010, **Zhao Lianhai**, le directeur du site Internet *Kidney Stone Babies*, dédié aux droits des enfants contaminés dans l'affaire du lait toxique, a été jugé à huis clos. Accusé d'avoir « occasionné des troubles », il est détenu depuis novembre 2009. Son verdict n'est pas encore connu.

http://fr.rsf.org/spip.php?page=article&id_article=36907

Thème: Cyber-espions…et les autres?

Theme: Cyber-spies…and the others?

N.B.: Le cyber-espionnage n'est pas unique à la Chine. Il est bon de placer le tout dans un contexte mondial. (MJK)

N.B.: Cyber-espionage is not unique to China. It is good to place it into a more global perspective. (MJK)

From: Guardian.co.uk
3 February 2010

Cyber-warfare 'is growing threat'

International Institute for Strategic Studies says cyber attacks could become weapon of choice in future conflicts

Simon Tisdall

Cyber-warfare attacks, such as the targeting of activists' emails in China recently, are a growing threat, according to security experts.

Cyber-warfare attacks on military infrastructure, government and communications systems, and financial markets pose a rapidly growing but little understood threat to international security and could become a decisive weapon of choice in future conflicts between states, the London-based International Institute for Strategic Studies warned yesterday.

IISS director-general John Chipman said: "Despite evidence of cyber attacks in recent political conflicts, there is little appreciation internationally of how to assess cyber-conflict. We are now, in relation to the problem of cyber-warfare, at the same stage of intellectual development as we were in the 1950s in relation to possible nuclear war."

The warning accompanied yesterday's publication of the Military Balance 2010, the IISS's annual assessment of global military capabilities and defence economics. The study also highlighted a

series of other security threats, including the war in Afghanistan, China's military diversification, the progress of Iran's suspect nuclear programme, and the impact of terrorist groups in Iraq and elsewhere.

Future state-on-state conflict, as well as conflicts involving non-state actors such as al-Qaida, would increasingly be characterised by reliance on asymmetric warfare techniques, chiefly cyber-warfare, Chipman said. Hostile governments could hide behind rapidly advancing technology to launch attacks undetected. And unlike conventional and nuclear arms, there were no agreed international controls on the use of cyber weapons.

"Cyber-warfare [may be used] to disable a country's infrastructure, meddle with the integrity of another country's internal military data, try to confuse its financial transactions or to accomplish any number of other possibly crippling aims," he said. Yet governments and national defence establishments at present have only limited ability to tell when they were under attack, by whom, and how they might respond.

Cyber-warfare typically involves the use of illegal exploitation methods on the internet, corruption or disruption of computer networks and software, hacking, computer forensics, and espionage. Reports of cyber-warfare attacks, government-sponsored or otherwise, are rising. Last month Google launched an investigation into cyber attacks allegedly originating in China that it said had targeted the email accounts of human rights activists.

In December the South Korean government reported an attack in which it said North Korean hackers may have stolen secret defence plans outlining the South Korean and US strategy in the event of war on the Korean peninsula. Last July, espionage protection agents in Germany said the country faced "extremely sophisticated" Chinese and Russian internet spying operations targeting industrial secrets and critical infrastructure such as Germany's power grid.

One of the most notorious cyber-warfare offensives to date took place in Estonia in 2007 when more than 1 million computers were used to jam government, business and media websites. The attacks, widely believed to have originated in Russia, coincided with a period of heightened bilateral political tension. They inflicted damage estimated in the tens of millions of euros of damage.

China last week accused the Obama administration of waging "online warfare" against Iran by recruiting a "hacker brigade" and manipulating social media such as Twitter and YouTube to stir up anti-government agitation.

The US Defence Department's Quadrennial Defence Review, published this week, also highlighted the rising threat posed by cyber-warfare on space-based surveillance and communications systems."On any given day, there are as many as 7 million DoD (Department of Defence) computers and telecommunications tools in use in 88 countries using thousands of war-fighting and support applications. The number of potential vulnerabilities, therefore, is staggering." the review said.

"Moreover, the speed of cyber attacks and the anonymity of cyberspace greatly favour the offence. This advantage is growing as hacker tools become cheaper and easier to employ by adversaries whose skills are growing in sophistication."

Defensive measures have already begun. Last June the Pentagon created US Cyber Command and Britain announced it was opening a cyber-security operations centre attached to GCHQ at Cheltenham, in coordination with MI5 and MI6.

William Lynn, US deputy defence secretary, described the cyber challenge as unprecedented. "Once the province of nations, the ability to destroy via cyber now also rests in the hands of small

groups and individuals: from terrorist groups to organised crime, hackers to industrial spies to foreign intelligence services … This is not some future threat. The cyber threat is here today, it is here now," Lynn said.

• The IISS 2010 Military Balance, published yesterday, said the insurgency in Afghanistan is complex and Pakistan's full cooperation remains elusive.

• Al-Qaida retains the capability to launch regular attacks in Baghdad.

• The report said technical difficulties frustrate Iran's nuclear ambitions but all the same Iran's stockpile of enriched uranium continues to grow.

• The IISS looked forward to increased defence co-operation between France and Britain,saying both countries needed to "spend smarter" because they cannot afford to "spend more".

http://www.guardian.co.uk/technology/2010/feb/03/cyber-warfare-growing-threat

---

Thème: Espionnage a d'autres formes

Theme: Espionage has many shapes

N.B.: Évidemment, les chinois n'emploient pas seulement le cyber-espionnage. Toutes les formes d'espionnage et d'ingérence sont utilisées. (MJK)

N.B.: Cyber-espionage is not unique to China. It is good to place it into a more global perspective. (MJK)

De : Intelligence Online
22 avril 2004

Pékin prend soin de ses taupes

Quand ils sont trop exposés, la Chine rapatrie sur son territoire les espions occidentaux que ses services ont retournés, et continue à les employer comme conseillers.

L'accident d'avion qui a décapité tout l'état-major polonais le 10 avril va reléguer à l'arrière-plan l'affaire d'espionnage dans laquelle se débat depuis plus d'un an le renseignement militaire polonais (**Sluzba Wywiadu Wojskowego** ou SWW). Un officier du SWW, **Stefan Zielonka**, a disparu en mai 2009. Il était très au fait des systèmes de chiffrage et de codage de l'**OTAN**, ainsi que des réseaux des services polonais à l'étranger. C'est la sécurité d'Etat chinoise (**Guoanbu**) qui aurait exfiltré Zielonka en Chine. A l'instar des Soviétiques pendant la guerre froide, Pékin opère un programme spécifique pour les transfuges occidentaux. Après avoir servi de taupes dans leur pays, ces anciens diplomates ou agents de renseignement sont relocalisés en Chine. Zielonka, le chiffreur polonais, aurait ainsi été installé dans la région de Shanghaï avec sa femme et son enfant, qui ont disparu peu de temps après lui. Une fois acclimatés, les transfuges ne cessent pas pour autant de travailler pour le renseignement chinois. Ils deviennent conseillers du département chargé d'espionner leur pays d'origine. Selon nos informations, plusieurs pays européens auraient ainsi "perdu" des éléments de leurs services de renseignement ces dernières années.

http://www.intelligenceonline.fr/article/free_article.aspx

N.B.: Cet article illustre des pratiques employées par le gouvernement chinois afin de maximiser l'utilisation des "amis" (Agents d'influence). Les politiciens et particulièrement les chefs d'État sont des plus utiles à cause des niveaux auxquels ils ont accès et leur influence. Pour se faire, l'utilisation d'agents qui peuvent fournir des fonds ou des avantages d'affaires sont des plus importants dans l'équation. (MJK)

N.B.: This article describes ways employed by the Chinese Government to maximize the use of "friends" (Agents of Influence). Elected officials and particularly current or ex-Head of State are the most useful due to their level of reach and influence. To assist, other agents that can provide funds or other business opportunities are very important in the equation. (MJK)

From;: The Asian Pacific Post
Feb. 19, 2004)

Chrétien hooks up with shady Chinese firm

By Asian Pacific News Service

After 10 years of building Canada as Beijings biggest western ally, former prime minister Jean Chrétien went to China this month to reap what he has sown on the taxpayers coin.

Less than two months after stepping down, Chrétien was hosted by the state-owned China International Trust and Investment Corp or CITIC which is the communist regimes most politically connected financial and industrial conglomerate.

According to a report from China, Chrétien was to meet CITICs top executives, travel to Shanghai and Shenyang, near the North Korean border under a veil of secrecy in a completely private visit.

The CITIC officials he met are expected to visit Canada later this year.

There is no doubt that he is trying to capitalize on his close relationship with China, said a B.C. based political analyst.

But there is something wrong with at least the optics here - he has gone to China at least six to eight times with Team Canada and as PM to facilitate huge business deals between China and Canada including some with CITIC and its subsidiaries.

The ink is hardly dry on his retirement papers and he is back there to do business again this time for himself, he said.

Chrétien's last visit to China was last November and among his last official duties was a formal meeting with Chinese Prime Minister Wen Jiabao on his final day in office on Dec. 12.

Wen sits on the Chinese executive body that oversees CITIC, whose operations have been the subject of intelligence reports in the U.S., U.K., Australia, and Canada.

CITIC's top dog is Wang Jun, a Chinese princeling who has been linked to everything from illegal arms shipments to illegal campaign donations in the United States.

With an estimated asset base of C$48 billion, CITIC is among the worlds largest corporations with 44 subsidiaries and banks including those in Hong Kong, the United States, Canada, Australia, New Zealand.

It has close links to the Peoples Liberation Army, counts among its advisors Chrétien's son-in-law Andre Desmarais of Power Corp and answers directly to Chinas top ruling echelon.

CITIC states its core business ranges from the financial industry, industrial investment to service industries and that it is a window to Chinas opening to the outside world. The respected U.S. based Rand Corporation, a non-profit research and analytical think-tank has another view.

In a 1997 report entitled, Chinese Military Commerce and U.S. National Security, the RAND Center for Asia Pacific Policy reported that CITIC acts as a shell or front operation on behalf of Chinas Peoples Liberation Army.

The report on CITIC noted that the Beijing-based investment firm had acted as a front for Poly Technologies Inc., an arms manufacturer owned directly by the Chinese army. According to the Rand Corporation report, Poly Technologies, Ltd., was founded in 1984, ostensibly as a subsidiary of CITIC, although it was later exposed to be the primary commercial arm of the PLA General Staff Departments Equipment Sub-Department. Throughout the 1980s, Poly sold hundreds of millions of dollars of largely surplus arms around the world, exporting to customers in Thailand, Burma, Iran, Pakistan, and the United States.

The report sponsored by the Clinton administration said CITIC is an investment concern under Chinas governmental State Council. CITIC became identified with the PLA as a result of the scandal surrounding Wang Jun and his visit to the White House on 6 February 1996.

The Rand report concluded: CITIC does enter into business partnerships with and provide logistical assistance to PLA and defense-industrial companies like Poly Technologies Inc.

Poly's U.S. subsidiaries were abruptly closed in August 1996, after federal US authorities in California concluded a lengthy sting operation by arresting seven people linked to Poly and another state-run Chinese arms firm for allegedly smuggling 2,000 AK-47 or Kalashnikov rifles into the country.

Had the sting operation continued, federal officials said at the time, more powerful weaponry and at least one senior Chinese official might have been lured to the United States.

After the operation Clinton said he made a mistake linking up with CITIC boss Wang Jun. Wangs background was apparently not scrutinized by the White House because he was brought there by long-time Clinton friend and campaign donor Charles Yah Lin Trie. Trie raised hundreds of thousands of dollars for Clintons Democratic party and for a legal defense fund established to help defray costs associated with several legal proceedings against the president.

Thousands of dollars for the legal defence fund, which came from Asian tycoons, ostensibly seeking to be friendly with the Clinton administration, were returned after an investigation into the origins of the money.

Another U.S. think-tank, The Center for Security Policy in a report to the U.S. Congress stated that CITIC - the corporate flagship of Chinas military-industrial complex with the wrong leadership, corporate history and agendas been attracting large sums of totally undisciplined cash from a wide spectrum of American investors.

The Casey Institute believes that the troubling national security aspects of CITICs established presence in the U.S. bond market should be explored, at a minimum, by the U.S. Senate Governmental Affairs and House Government Reform and Oversight Committees.

Yet another American report, this time by The United States House of Representatives Select Committee on U.S. National Security and Military/Commercial Concerns with the Peoples Republic of China described CITICs Wang Jun as having been directly involved in illegal activities in the United States.

Commonly known as the Cox report, the study described Wang Jun as the son of the late Chinese President Wang Zhen and a notable princeling whose family ties and personal connections are able to cross the lines and accomplish things that might not otherwise be possible.

It was not only the Americans who were sounding the warnings on CITIC and Chinese front companies in the mid-nineties.

In Canada, a small team of RCMP and CSIS officials were also at that time putting together a highly controversial report dubbed Sidewinder, which would be eventually snubbed by Chrétien's China-friendly cabinet as a rumour laced conspiracy theory. Sidewinder stated: China remains one of the greatest ongoing threats to Canada's national security and Canadian industry.

There is no longer any doubt that the Chinese Intelligence Service has been able to gain influence on important sectors of the Canadian economy, including . . . real estate, high technology, security and many others. In turn, it gave them access to economic, political and some military intelligence of Canada.

The report, whose official title is Chinese Intelligence Services and Triads Financial Links in Canada, was supposed to be destroyed after CSIS officials decided to tone down the conclusions in a revised document called Echo.

CSIS officials have insisted Sidewinder was buried because it was nothing more than conspiracy theories. (See www.asianpacificpost.com, August 7 - August 20, 2003, 3,500 Chinese spy companies identified in Canada and U.S.)

Other intelligence sources say political pressure forced CSIS to hush the Sidewinder report.

Among Sidewinder's case studies were CITIC. It stated among other issues that:

i) The Chinese, state-owned China International Trust Investment & Company (CITIC), which has a subsidiary in Canada, has spent about $500 million to buy a Canadian pulp mill, petrochemical company, real estate and hotels. CITIC also has connections with at least one large Canadian corporation.
ii) Large amounts of arms manufactured by a CITIC-controlled company have been confiscated on Mohawk reserves.
iii) Chinese tycoons and CITIC own large chunks of real estate and hotel chains in key urban centres, giving them great influence in local politics and development.

CITIC is also closely connected to Chinas state-owned COSCO shipping company, which uses

Vancouver as its North American gateway.

U.S. Senate and Canadian intelligence officials have described COSCO as the merchant marine for Chinas military.

COSCO vessels have been caught carrying assault rifles into California and Chinese missile technology and biological-chemical weapons components into North Korea, Pakistan, Iraq and Iran, according to U.S. intelligence reports.

In addition, Canadian law enforcement agencies have warned that Chinese Triad criminal organizations are active in and around Canada's ports.

Another tycoon closely affiliated to CITIC is Li Ka Shing - also a Sidewinder target and Asia's most powerful man. He owns large tracts of real estate in Canada and interests in the country's telecommunications, petroleum and banking sectors.

The Royal Hong Kong Police asked CSIS to investigate Li here in Canada in 1988, just as he was acquiring Vancouver's Expo 86 lands, but the request was officially denied by then Canadian High Commissioner to Hong Kong Anne-Marie Doyle.

U.S. Congressman Dana Rohrabacher said, The U.S. Bureau of Export Affairs, the U.S. Embassy in Beijing and the Rand Corporation ... have identified Li Ka Shing and Hutchison Whampoa (Li's primary business) as financing or serving as a conduit for Communist Chinas military for them to acquire sensitive technologies and other equipment.

Chrétien, during his brief sojourn from politics while John Turner was leader of the federal Liberals, worked for Gordon Securities - one of the many Li-controlled companies in Canada.

Chrétien's connections to the shady CITIC conglomerate is not the only foray by the former prime minister into the world of business.

Among his other ventures include a gig as an international-relations adviser to PetroKazakhstan, a Calgary-based oil company that is trying to expand its oil exports to China.

James Grier, a China watcher, said Chrétien's involvement with CITIC does raise eyebrows.

There is a volume of history with this company that could impact the stature of someone like Chrétien, but from what we know that seems to have little impact on Chrétien, he said.

Grier said, given the current sponsorship scandal plaguing the Liberals, the party could take another serious blow if anyone from their top echelon is found to have a direct benefit in China from their last days in office.

http://www.primetimecrime.com/APNS/20040219.htm

From: New America
27 April 2010-04-29

Chinese Spying in United States

A secret FBI videotape showing the transfer of classified military documents to a communist

Chinese agent was released in February to the world, providing a brief peek at the shadowy world of espionage against America. Pentagon analyst Gregg Bergersen with the Defense Security Cooperation Agency is shown receiving a wad of bills and telling People's Republic of China spy Tai Shen Kuo that he's "very reticent" to let him have the information "because it's all classified."

The documents included sensitive material about weapons sales to Taiwan — a U.S. ally, which the communist regime considers a breakaway province to be conquered eventually — and details of a communications system. Bergersen told Kuo: "You can take all the notes you want … but if it ever fell into the wrong hands … then I would be fired for sure. I'd go to jail because I violated all the rules." He was eventually convicted and sentenced to five years, while Kuo received a 15-year sentence. The investigation also identified other sources who were providing secrets about American space and naval technology to the PRC.

In February, another Chinese spy was sentenced to 15 years in jail for stealing sensitive secrets from his former employers — Boeing and Rockwell International — and passing them to the communist regime. Engineer Dongfan "Greg" Chung reportedly gave up trade secrets about American space shuttles, military aircraft, and even the Delta IV rocket. Though Chung was 73 years old, the judge said he handed out the possible life sentence as a message to the Chinese government: "Stop sending your spies here."

Chung was reportedly aided in his crimes by Chi Mak, a former defense-contractor engineer. Mak was convicted of conspiring to pass sensitive military technology to the PRC, including information on Navy ships, nuclear submarines, and more. "We will never know the full extent of the damage that Mr. Mak has done to our national security," wrote the judge, who sentenced Mak to 24 years. His family later pled guilty to related criminal charges.

These are just a few of the more recently convicted PRC spies operating in the United States. The FBI has arrested dozens of Chinese on American soil in recent years for involvement in espionage operations on behalf of the communist regime. And according to various reports, there are close to 500 similar investigations ongoing. The problem is indeed enormous.

Extent and Methods of Spying

Of course, the Chinese government vehemently denies that it is engaged in espionage. "Some people have always favored making up Chinese spy stories for sensationalism," PRC Foreign Ministry spokesperson Ma Zhaoxu told reporters after the sentencing of Dongfan "Greg" Chung for espionage.

Other communist officials claim that the accusations of spying are designed to "defame China." Peng Bo with the "Internet Bureau" of the Chinese Information Office denied involvement in recent cyber attacks blamed on the regime: "The government has never supported or been involved in cyber attacks, and it will never do so," he told the state-run Xinhua, adding that the charges were "sheer nonsense" and "groundless." But nobody really believes that, not any more than they believe Chairman Mao was an "agrarian reformer."

French author Roger Faligot, who has written dozens of espionage-related books, including The Chinese Secret Services From Mao to the Olympic Games, claims there are some two million Chinese spies working with the communist state's security apparatus. The regime has countless agencies engaged in intelligence gathering, including the Ministry of State Security; various military intelligence agencies; multiple industrial, political, and economic espionage departments; and more.

Hiding behind "diplomatic immunity" and using blackmail, bribery, special privileges, strategic "business" partnerships, cyber attacks, and a wide array of other methods, China's spies have been extremely successful in their efforts.

“The Chinese are the biggest problem we have with respect to the level of effort that they’re devoting against us versus the level of attention we are giving to them,” former U.S. counterintelligence chief Michelle Van Cleave told CBS, explaining that it was impossible to know the true magnitude of the problem. And she isn’t the only concerned American official.

In its 2007 annual report to Congress on the military power of the PRC, the Department of Defense explained that Chinese espionage is a critical threat. “Several high profile legal cases highlight China’s efforts to obtain sensitive U.S. technologies (e.g., missile, imaging, semiconductor, and submarine) illegally by targeting well-placed scientists and businessmen,” explained the report. “U.S. Immigration and Customs Enforcement (ICE) officials have rated China’s aggressive and wide-ranging espionage as the leading threat to U.S. technology. Since 2000, ICE has initiated more than 400 investigations involving the illicit export of U.S. arms and technologies to China.”

American military and government-related intelligence is one of the top priorities for Chinese intelligence services. Fengzhi Li, a former spy recruiter for the communist regime who defected and is now seeking asylum in the United States, told CBS’ 60 Minutes that “without a doubt,” China’s Ministry of State Security dedicates most of its efforts to spying on America.

Chinese espionage against the U.S. military goes back a long way, too. It has even been aided in recent decades by some top American officials, including a former U.S. President. Bill Clinton helped the hostile communist government access some of the most sensitive American military technology while covering up various crimes for the regime and its agents. As documented in the February 15, 1999 “Chinagate: Treason in the White House” issue of The New American, Clinton’s collaboration was secured in exchange for massive unlawful campaign contributions.

“President Clinton promised to restrain those who ordered the Tiananmen Square massacre, but he has now allowed these men whose hands are stained with the blood of martyrs of freedom into the highest reaches of our military defenses, and made available to them significant portions of our advanced military technology,” wrote former Joint Chiefs of Staff Chairman Admiral Thomas Moorer.

Chinese espionage against the U.S. government and armed forces has been so successful that it may seem there cannot be a whole lot left for the regime to steal. A late-1990s congressional committee found that the Chinese regime already possessed vast amounts of America’s most sensitive military information, including the designs of American thermonuclear weapons.

But military and government secrets aren’t the only things the regime is seeking. Economic espionage has become a huge drain on the American economy. “The Cold War isn’t over, it has just moved into a new arena: the global marketplace,” notes the FBI on its website. The agency estimates that “every year billions of U.S. dollars are lost to foreign competitors who deliberately target economic intelligence in flourishing U.S. industries and technologies, and who cull intelligence out of shelved technologies by exploiting open source and classified information known as trade secrets.” Current estimates on the cost of economic espionage to U.S. businesses are difficult to find, but FBI Director Robert Mueller told the Detroit Economic Club in 2003 that “theft of trade secrets and critical technologies — what we call economic espionage — costs our nation upwards of $250 billion a year.” And China is the main problem.

The examples of Chinese economic espionage aren’t new either. From spying on American

firms in Silicon Valley to stealing proprietary software from foreign firms in China, the regime does it all. Some analysts, like cyber-security expert Alan Paller of the SANS (SysAdmin, Audit, Network, Security) Institute, claim that every foreign company with operations in China has probably had its computer networks compromised by the communist government.

Earlier this year, the family-owned American software firm Cybersitter initiated a federal lawsuit against the PRC and two contractors for stealing its proprietary anti-pornography software. The regime used it to censor the Internet in China. “I don’t think I have ever seen such clear-cut stealing,” said an attorney for the company. The estimated damages to Cybersitter: over $2 billion.

Then there is the spying on dissidents. Owing to the totalitarian nature of the Chinese regime, countless people have fled the country. But it turns out they aren’t safe no matter where they go. Fengzhi Li, the former Chinese intelligence officer who defected and is seeking asylum in the United States, told a news conference last year after speaking before Congress that the communist government spies on spiritual groups, dissidents, and “aggrieved poor people” overseas.

Former Chinese diplomat Chen Yonglin, who was based in Australia and also recently defected, told New Tang Dynasty Television about some of the methods used by the communist regime to control Chinese populations abroad in order to further communist aims. These include setting up “fake” umbrella organizations to create the illusion that all Chinese living outside China think like the Chinese Communist Party. He said officials would send students and other spies to Chinese human-rights demonstrations to act as agents provocateurs and compile lists of who attended.

“Basically, the Chinese student organization in every school is under [Chinese Communist Party] control, other than the ones started by individuals with views that disagree with the CCP’s,” he said. “Their operation funds mostly come from the education department of the consulate, and meetings are held on consulate grounds. The representatives and the chair persons in the student organizations are appointed by the consulate.” Many of the groups’ websites even openly acknowledge the connection.

In his tenure as a high-level Chinese diplomat in Australia, Yonglin spent much of his time keeping tabs on Falun Gong practitioners and waging a propaganda war against them. He revealed that there was a 1,000-member-strong Chinese spy network operating in the country.

Indeed, the regime expends a great deal of effort spying on Chinese dissidents in Europe as well. In early March, a Swedish court convicted Babur Maihesuti of aggravated illegal espionage against members of the persecuted Chinese-minority Uighur community exiled in Sweden. According to the court, he gathered information regarding the travel habits, health, refugee status, and political inclination of Uighurs and transferred it to the communist regime.

One of the most serious espionage threats from the Chinese government is found on college campuses, according to experts, officials, and defectors. There are an estimated 150,000 Chinese students studying at American universities, according to Time magazine. And according to officials, the institutions are a prime target for spies seeking sensitive technological information. Of course, not all Chinese students in America are here to spy or steal information. Many of them are here in search of a better life away from the pervasive thumb of communist authoritarianism. But not all of them. According to a survey by China’s official news organ, 81 percent of Chinese students in America plan to return home after receiving their U.S. education.

“Everything that’s needed for a modern industrial military state is leaving here, and going

there," University of Michigan aerospace engineering professor Bill Kauffman explained in a video interview with investigative reporter Vince Wade about the problem.

Ultimate Goals

So what are the aims of the communist regime's espionage activities? Different experts interviewed by The New American for this story expressed various opinions, but none of the theories are good.

"The Chinese are assembling a comprehensive 'map' of the U.S. government and economy while simultaneously looting our high technology for their own industrial and economic purposes," explained Charles Viar, a former U.S. counterintelligence official and the chair of the Center for Intelligence Studies. The goal, he said, is "to achieve international hegemony — peacefully, if possible. At minimal military cost if not."

"The Chinese are moving forward with building an aircraft carrier, they're establishing ports all over, and advanced missile systems and satellite systems," said Roger Canfield, Ph.D., author of several books on the Chinese regime and its espionage operations, including China's Trojan Horses: Red Chinese Soldiers, Sailors, Students, Scientists and Spies Occupy America's Homeland. He told The New American that the long-term goal was military modernization on a scale that would someday be able to challenge American power.

Chinese dissidents who have experienced the regime's brutality are acutely aware of the possibilities for danger. "The Communist Party wants to survive, and it will steal for survival — it's self-interest," explained Samuel Zhou, the executive vice president of New Tang Dynasty Television and a native-born Chinese who emigrated to America after the Tiananmen Square massacre. In an interview with The New American, he explained: "They need to grow the economy to defend themselves from the mass[es] … so they need economic information. And then there's Taiwan of course.... Whether they have the power to conquer the world — that's still far away. But they do want to have at least this kind of control — they want to control others, and once they have this information, they have ways to manipulate people.... I don't want to make a prediction now, but communism is communism — they have no principles. If they can kill tens of millions of their own people, what could they do to the world? It's kind of obvious."

Former Canadian Minister of Parliament David Kilgour, also a former Minister of State for the Asia-Pacific region, put it bluntly. "There's absolutely no doubt that their long term goal is world domination and to put the United States — as much as they can — out of business, and to become the world's superpower," he told The New American. "They want to run the whole planet."

And indeed, the communist government has given good indications of their way of thinking. Top Chinese military officials have openly discussed destroying American cities with nuclear weapons, especially if the United States intervenes militarily on behalf of Taiwan. "If the Americans draw their missiles and position-guided ammunition on to the target zone on China's territory, I think we will have to respond with nuclear weapons," said Chinese Major General Zhu Chenghu in a speech. "We Chinese will prepare ourselves for the destruction of all of the cities east of Xian. Of course, the Americans will have to be prepared that hundreds of cities will be destroyed by the Chinese."

What It All Means

Most of the analysts who discussed with The New American the effectiveness of law enforcement and counterintelligence agreed that the U.S. government was not doing enough to counter the threat. "American counterespionage — the FBI — has been largely ineffective against the Chinese and, indeed, the Chinese have twice managed to suborn FBI agents deployed against them (using sexual lures)," said Charles Viar of the Center for Intelligence

Studies in an e-mail to The New American. In its recommendations to Congress, the U.S.-China Economic and Security Review Commission suggested an assessment of export control enforcement and counterintelligence efforts, and possibly providing more funding for operations to prevent illicit technology transfer to the regime or its industrial espionage programs. It also recommended a review of American military and intelligence computer networks.

Some of the methods suggested by experts interviewed for this story include properly vetting Chinese students aiming to study in American universities, tightening export controls on sensitive technology, and actively enforcing the restrictions, among others proposals. Increasing resources to counterespionage programs would help, too.

http://www.thenewamerican.com/index.php/usnews/crime/3404-chinese-spying-in-the-united-states