Industrial Espionage[1]

by M. E. Kabay, PhD, CISSP-ISSMP[2]

Contents

[1] This article is an edited compilation of a series originally published in the *Network World Fusion Security Newsletter* in 2005. Archives at < http://www.nwfusion.com/newsletters/sec/index.html >. Updated January 2008 for publication in *Vacuum & Coating Technology*.

[2] CTO & MSIA Program Director / School of Graduate Studies / Norwich University, Northfield VT, USA 05663-1035. Web site < http://www2.norwich.edu/mkabay >.

Industrial Espionage

Introduction

One of the problems we face in our field of information assurance is the paucity of credible data about threats to our systems. We suffer from problems of ascertainment and problems of data collection in this field; without going into details here, there is plenty of reason to believe that we do not notice many of the system intrusions that take place and that many of those that are noticed are not reported in a way that allows development of a statistical base.[3]

The US National Counterintelligence Center (NACIC) which later became the Office of the National Counterintelligence Executive (ONCIX) have been reporting annually to Congress since 1995 about foreign economic collection and industrial espionage.[4] There are some valuable findings and trends in industrial espionage that can help us interfere with industrial spies.

First of all, Section 809 of the US Intelligence Authorization Act for Fiscal Year 1995 defined foreign industrial espionage as "industrial espionage conducted by a foreign government or by a foreign company with direct assistance of a foreign government against a private United States company and aimed at obtaining commercial secrets."[5]. Throughout the decade of reporting, there has been little change in the list of targeted technologies; the 2004 report lists the following: Information systems are a key target, with more than 40% of the PhDs employed in the field in 2001 (the most recent year of available data) being foreign-born (compared with 10% of all PhD scientists and engineers overall in the USA). Sensors, aeronautics, electronics, armaments and energetic materials are other industrial targets for espionage. The 1996 report notably added biotechnology, information warfare, manufacturing processes, nuclear systems, space systems, telecommunications and weapons effects and countermeasures to the list of targets.

[3]Kabay (2007)
[4]Some archival NACIC and current ONCIX reports are freely available as PDF files from < http://www.ncix.gov/publications/reports/index.html >..
[5] NACIC (1995) report, p. 1

Methods

Industrial espionage is carried out in many ways. The 1995 NACIC report lists the following:

- Traditional methods of espionage include classic agent recruitment, US volunteers,[6] surveillance, surreptitious entry (including bribery at hotels to allow access to guest and luggage rooms), specialized technical operations (e.g., communications intelligence and signals intelligence – COMINT and SIGINT) and economic disinformation (DISINFO and psychological operations – PSYOPS).

- Additional methods include using foreign students studying in the USA, foreign employees of US firms and agencies, debriefing foreign visitors to the USA on their return to their home country, recruitment of émigrés, ethnic targeting (suborning or threatening Americans with foreign family ties), and elicitation during international conferences and trade fairs. Agents have also exploited private-sector firms, joint ventures, mergers or acquisitions and non-profit organizations as opportunities and fronts for espionage. Hiring competitors' employees, signing corporate technology agreements, sponsoring research projects in the USA and assigning foreign liaison officers to government-to-government research and development projects are additional valuable methods for covert data gathering.

- Open-source intelligence (OSINT) methods include open or covert use of public databases, hiring information brokers and assigning consultants to gather information for confidential research reports. In some cases foreign interests have paid lobbyists to influence lawmakers and to facilitate extended contacts with high-placed officials with access to valuable information. Other OSINT channels listed in the 1996 report include bid proposals, energy policies, marketing plans, price structuring, proposed legislation, tax and monetary policies, and control regulations for technology transfer and munitions.

The 2000 NACIC added these methods:

- Requesting information through e-mail or letters, including apparent responses to advertising or trade show exhibits.

- Exploiting Internet discussion groups, especially research-oriented list servers.

A survey organized by NACIC among about a dozen Fortune 500 company officers extended the list of industrial espionage methods with the following approaches:

- Breaking away from tour groups
- Attempting access after normal working hours
- Supplying different personnel at the last minute for agreed-upon projects

[6] See the ONCIX "One Evil" awareness poster
< http://www.ncix.gov/publications/posters/poster_oneevil.html >

- Theft of laptops
- Customs holding laptops for a period of time
- Social gatherings
- Dumpster® diving (searching through trash and discarded materials)
- Intercepting nonencrypted Internet messages.[7]

I want to make it clear that the NACIC/ONCIX authors and I as a writer reporting on their findings are *not* implying that foreign nationals and foreign-born citizens in the USA are inherently threats to national security. The vast majority of such people – and I was one myself, having been born in Canada and having been granted US citizenship in July of 2005 – are honest, loyal people who have never done anything against the interests of our country. The US Census Bureau reports that in 2004, there were over 34 million foreign-born residents [8] out of a total population estimated at over 293 million.[9] So even if we guessed there were a thousand foreign-born spies (a high estimate for which there is no factual basis whatsoever), that number would represent a mere 0.003% of the foreign-born population – leaving 99.997% as unworthy of suspicion. So the next time someone tries to convince you that purely ethnic profiling divorced from any study of individual behavior is a good idea for law enforcement and national security, do a similar calculation with them and calculate the costs of resources wasted on false-positives.

The NACIC/ONCIX reports are clear on the threat from purely domestic, All-American citizens: "In 1996, the FBI and ASIS also reaffirmed the increase in the reporting of domestic theft or misappropriation of proprietary economic information. An ASIS special report released in March 1996, *Trends in Intellectual Property Loss*, indicated that 74 percent of intellectual or proprietary property losses stemmed from the actions of ''trusted relationships'' – employees, former employees, contractors, suppliers, and so forth."[10]

An additional source of information is the *Annual Report to Congress on Military Power of the People's Republic of China 2007*.[11] Chapter Five, "Resources for Force Modernization," reports that "China's defense industries benefit from foreign direct investment and joint ventures in the civilian sector, technical knowledge and expertise of students returned from abroad, and state-sponsored industrial espionage." Later in the report, the authors add, "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."

[7] NACIC Report (2000) p. 16
[8] Bernstein (2005)
[9]U. S. Census Bureau (2005). MS-Excel file
[10] NACIC Report (1996), p. 5
[11] US Secretary of Defense (2007). Annual Report to Congress, Chapter 5.

Survey Data & US Government Reports

In 1995, the American Society for Industrial Security [12] ran a survey that was used by NACIC in its 1995 report. Among the significant findings were the following (quoting NACIC but adding bullets):

- Reported incidents increased 323 percent since 1992.
- Losses of corporate information increased from a reported 9.9 incidents per month in 1992 to an average of 32 incidents per month in 1995.
- About three-fourths of reported losses occurred in the United States, and the majority of those incidents involved ‘‘trusted relationships’’ (employees, vendors, contractors, retirees, and so forth).
- Other incidents were attributable to a variety of sources: domestic competitors, computer hackers, foreign competitors, foreign intelligence services, and foreign business partners.
- Of incidents outside the United States, approximately half took place in countries traditionally considered allies of the United States.
- Foreign nationals were identified in 21 percent of the incidents where the perpetrator’s nationality was known.

The 1997 NACIC report cited work by the Computer Security Institute [13] in cooperation with the FBI’s International Computer Crime Squad in San Francisco. Interesting results included the following (bullets added to verbatim quotes):

- According to the survey, about 75 percent of the 563 responding corporations, government agencies, financial institutions and universities surveyed by CSI reported financial losses in the past 12 months.
- [In 1996] financial losses from financial fraud, computer viruses, sabotage, and theft of proprietary information and laptops were up seven percent and topped $100 million. Reflecting the increased competition in the global marketplace, over 50 percent of the respondents cited foreign competitors as a likely source of attack and 22 percent cited foreign governments as a likely source of attack.
- The survey also showed that only 17 percent of the respondents reported crimes to law enforcement authorities. There appears to be reluctance on the part of the private sector to report allegations of computer and economic crime to law enforcement authorities. A large number of these crimes go unreported because of a company’s fear of undermining the confidence of their shareholders, negative publicity, and further exposure of trade secret information during prosecution.

In 1998, NACIC reported on a then-new economic modeling tool developed at the Department of Energy’s Pacific Northwest National Laboratory (PNNL) that was applied to a single case of theft of intellectual property in which a foreign competitor succeeded in capturing the market

[12] ASIS – American Society for Industrial Security International
< http://www.asisonline.org >
[13] CSI – Computer Security Institute
< http://www.gocsi.com >

due to the theft. "Using this tool, the misappropriation of intellectual property in this case resulted in over $600 million in lost sales, the direct loss of 2,600 full-time jobs, and a resulting loss of 9,542 jobs for the economy as a whole over a 14-year time frame. Analysis also determined that the US trade balance was negatively impacted by $714 million and lost tax revenues totaled $129 million."

The "10th Annual Trends in Proprietary Information Loss Survey" [14] organized by ASIS reported that respondents in 138 companies in the Fortune 1,000 and from the US Chamber of Commerce membership list experienced losses totaling over $50B. About 40% of the respondents reported industrial espionage incidents during the period July 1, 2000 to June 30, 2001. The Executive Summary (pages 1-2) summarizes the risk factors and impacts of loss as follows:

RISK FACTORS

- The greatest risk factors associated with the loss of proprietary information and intellectual property among all companies responding were former employees, foreign competitors, on-site contractors, and domestic competitors. Hackers also were cited as a major concern among some sectors.
- The most commonly cited areas of risk by companies that reported an incident were: research and development (49%), customer lists and related data (36%), and financial data (27%).
- The number of reported incidents, in order of magnitude, were: 1) customer data, 2) strategic plans, 3) financial data, and 4) R&D.

IMPACT OF LOSS

- Among all companies, the greatest impacts of proprietary information loss were increased legal fees and loss of revenue. For large companies (over $15 billion), loss of competitive advantage was the most serious problem. For financial firms, embarrassment was the biggest concern; and for high technology companies, the major issue was loss of competitive advantage.
- The assessment or assignment of intellectual property value is the responsibility of in-house patent and legal counsel who base their judgments on competitive advantage, profitability, and research and development criteria.

The National Counterintelligence Center (NACIC) later became the Office of the National Counterintelligence Executive (ONCIX). In 2004, the ONCIX reported to Congress that

- "… a recent private US survey indicated that more than half of the impacted firms do not report the breach for fear of reducing shareholder value. As a result, no one is certain how much technology and sensitive proprietary information are lost annually to cyber theft."
- "During FY2004, the US Department of Immigrations and Customs Enforcement (ICE) conducted more than 2,500 export investigations involving violations of the Arms Export Control Act, International Traffic in Arms Regulations (ITAR), Export Administration

[14] ASIS Report (2002)

> Regulations (EAR), Inter national Emergency Economic Powers Act, and the Trading With the Enemy Act. These investigations resulted in 146 arrests, 97 criminal indictments, and 79 criminal convictions."

Early reports from NACIC/ONCIX blanked out the names of countries suspected or known to be engaging in foreign industrial espionage against the USA; however, later editions began publishing lists. The countries mentioned in early reports were Algeria, Armenia, Azerbaijan, Belarus, China, Cuba, Georgia, India, Iran, Iraq, Israel, Kazakhstan, Kyrgyzstan, Libya, Moldova, Pakistan, Russia, Syria, Taiwan, Turkmenistan, Ukraine, and Uzbekistan.

In the 2000 Annual Report, respondents to the NACIC survey of a few (about a dozen) Fortune 500 companies reported that the top countries involved in industrial espionage cases involving their firms were (in order of importance) China, Japan, Israel, France, Korea, Taiwan, and India.

By 2002, the ONCIX Annual Report commented, "The laundry list of countries seeking US technologies in 2001 was long and diverse. Some 75 countries were involved in one or more suspicious incidents. The most active countries in economic espionage, according to DSS data, were an interesting mix of rich and poor and "friend" and foe. Many of the richest nations aggressively sought the latest in advanced technologies both to upgrade their already formidable military infrastructures—particularly command, control, and communications—and to make their already sophisticated industries even more competitive with the United States. Most of the poorer countries, however, continued to exhibit a preference for older 'off the shelf' hardware and software to renovate their existing defensive systems and to develop countermeasures to provide them battlefield advantage. The search for lower technology goods by these less developed countries probably reflected their desire to bring in technologies that could be more easily integrated into their existing military structures; a number of these countries were probably not capable of utilizing the most sophisticated US technologies."

In January 2005, the US Committee on Foreign Investments expressed "concern that Chinese operatives might use an IBM facility for industrial espionage."[15]

Agents

There is some information available about the people who become industrial spies.

The 2003 ONCIX report stated, "Foreigners from almost 90 countries attempted to acquire sensitive technologies from the United States in 2003, according to data compiled from across the [counterintelligence community], about the same number as in 2002." That report also explained, "While foreign government officials were behind some of the incidents, they by no means accounted for the majority of collection attempts. For example, Defense Security Service (DSS) data show that [bullets added]

[15] Spooner (2005)

- only about 15 percent of suspicious efforts to illegally acquire sensitive US military-related technology in 2003 directly involved foreign governments.
- Another 25 percent came from government-affiliated organizations or foreign companies that work solely or predominantly for foreign governments, according to DSS statistics.
- The remainder came from individuals (14 percent) claiming to be working for themselves and
- from company representatives (31 percent);
- in 15 percent of cases, there was no indication of affiliation."

According to the latest ONCIX report available (2004), "Individuals from both the private and public sectors in almost 100 countries attempted to illegally acquire US technologies in FY2004, roughly the same number of countries as [in 2003]…." However, the report indicates a possible growth in government-sponsored industrial espionage: "foreign state actors accounted for about one-fifth of suspicious incidents and government-related organizations accounted for another 15 percent." However, "Commercial organizations and private individuals with no known affiliation to foreign governments together accounted for nearly half—36 percent and 12 per cent respectively—of all suspicious incidents. In another 16 percent, the contractors were unable to determine the affiliation of the foreign parties involved in the elicitation."

In summary, the enormous investment in US intellectual property has been a prime target for nations and firms eager to find shortcuts in the research and development process and thus to reduce their costs by stealing our information.

Specific Cases

In this section, I review some interesting specific cases of industrial espionage from these government reports and others. I am summarizing and paraphrasing liberally to keep the length manageable and have deliberately not used quotation marks and ellipses to avoid cluttering the text. All of the information comes either from the NACIC/ONCIX reports, from my INFOSEC Year in Review database or from reports on Web sites for various offices of US Attorneys around the country.[16]

- Standard Duplicating Machines Corporation (SDMC) was the victim of unauthorized intrusion by a disgruntled former employee into a voice-mail system. John Hebel was employed by SDMC as a field sales manager from 1990 to 1992 when his employment was terminated. Hebel was subsequently hired by the US affiliate of Manufacturing Corporation of Japan (Duplo), the main competitor of SDMC. Through an unsolicited phone call from a customer, SDMC discovered that Hebel accessed SDMC's voice-mail and used the information to Duplo's benefit. Hebel was charged with one count of violating 18 USC §1343 (Wire Fraud) and on 14 March 1997, he was sentenced to two years probation. In addition, a civil suit brought against Duplo had a final settlement close to $1 million in SDMC's favor.

[16] Kabay (1994-2006)

- Harold Worden retired from Eastman Kodak in Rochester, NY after 30 years of service in the mid 1990s. He founded a consulting firm that hired up to 60 other Kodak retirees and proceeded to try to sell information gleaned from thousands of stolen confidential documents about Kodak's top-secret acetate-manufacturing machine. Both Agfa and Konica, competitors of Kodak approached by Worden, informed Kodak and the FBI of the attempts. In August 1997, Worden pleaded guilty to one count of interstate transportation of stolen property and went to jail for 15 months as well as having to pay a $30,000 fine. Kodak also sued him in civil court for damages.

- Patrick Worthing and his brother Daniel tried to sell confidential information from Pittsburgh Plate Glass Industries (PPG) information for $1,000 to an FBI Special Agent posing as a representative of Owen-Corning (OC), a major competitor. This was a particularly interesting case because OC reported the attempted sale of stolen data to PPG at once and fully cooperated with PPG and the FBI in capturing the thieves. Both subjects were and convicted under 18 USC Section 1832 (Theft of Trade Secrets) in April and June 1997. Daniel Worthing was sentenced to six months of home confinement, five years probation, and 100 hours of community service whereas Patrick Worthing was sentenced to 15 months in jail and three years probation.

- On 14 June 1997, Hsu Kai-Lo and Chester H. Ho (naturalized US citizens) were arrested by the FBI for attempting to steal the formula for Taxol, a cancer drug patented and licensed by the Bristol-Myers Squibb (BMS) Company presumably on behalf of their employer, the Yuen Foong Paper Manufacturing Company of Taiwan. In July 1997 the two accused along with Jessica Chou (a Taiwan citizen actively involved in the attempted theft) were indicted on 11 counts including violations of 18 USC Section 1832. Chou remained in Taiwan and that nation refused to extradite Chou.

- In September 1997, Pin Yen Yang and his daughter Hwei Chen Yang (a.k.a. Sally Yang) were arrested with Dr Ten Hong Lee for trying to steal valuable industrial secrets from the Avery Dennison Corporation (ADC), Pasadena, California, for transfer to the Four Pillars Company in Taiwan. Dr Lee, a Taiwan native and US citizen, had been an Avery Dennison employee since 1986 at the company's Concord, Ohio, facility. Dr Lee allegedly received between $150,000 and $160,000 from Four Pillars and Pin Yen Yang for his involvement in the illegal transfer of ADC's proprietary manufacturing information and research data over a period of approximately eight years. Economic losses to ADC were estimated at $50-60 million. This case marked the first conviction of foreign individuals or a foreign company under the Economic Espionage Act of 1996. On 5 January 2000, a Youngstown, Ohio, federal judge sentenced Pen Yen Yang to two years probation along with six months of home detention; Hwei Chen Yang was sentenced to one-year probation. Four Pillars was fined $5 million by a US District Court for accepting the pilfered secrets. Moreover, in February 2000, a jury verdict in US District Court, Cleveland ruled in favor of ADC in a civil case against Four Pillars and the judge awarded $80 million in damages.

- In 1997 John Fulton, a former employee of the Joy Mining Machinery, a global coal mining company approached a Joy employee in an attempt to purchase schematics for

part of the company's proprietary equipment. The Joy employee reported the attempt and worked with the FBI and his employer to record conversations in which Fulton offered to pay any amount of money for information pertaining to the specific equipment. On 21 November 1997, Fulton paid the cooperating witness $1,500 for blueprints and a technical binder, both of which were Joy proprietary items. Fulton was arrested by the FBI after the exchange and was charged with unlawfully attempting to obtain trade secrets (18 USC Section 1832). On 14 April 1998, Fulton pled guilty to one count of theft of trade secrets and was sentenced in September 1998.

- On 23 January 1998, Steven Louis Davis pled guilty to federal charges that he stole and disclosed trade secrets concerning a new shaving system developed by the Gillette Company. Davis was employed by Wright Industries, a subcontractor of Gillette Company, which had been hired to assist in the development of the new shaving system. In February and March 1997, Davis made disclosures of technical drawings to Gillette's competitors Warner-Lambert Co., Bic, and American Safety Razor Co. The disclosures were made by facsimile and electronic mail. Although the FBI is aware that Davis reached out to one foreign-owned company (Bic), it is unclear if he was successful in disseminating trade secrets overseas. Davis was arrested on 3 October 1997 and was indicted on counts of violating 18 USC Section 1343 (Wire Fraud) and 18 USC Section 1832 (Theft of Trade Secrets). On 17 April 1998, Davis was sentenced to two years and three months in federal prison.

- On April 26, 2001, Junsheng Wang of Bell Imaging Technologies pled guilty to violation of 18 USC 132(a)(2) by stealing trade secrets from Acuson Corporation. The Counterintelligence News and Developments (CIND) report noted, "In pleading guilty, Wang admitted that prior to August 24, 2000, that he took without authorization and copied for Bell Imaging a document providing the architecture for the Sequoia ultrasound machine that contained the trade secrets of Acuson Corporation. According to Wang's plea agreement, he had been able to obtain access to the Acuson trade secret materials because his wife was employed as an engineer at that company and because she had brought that document into their home. After he had copied the document, he took it with him on business trips to the People's Republic of China, turning it over to Bell Imaging during 2000."[17]

- In May 2001, NewsScan [18] reported that "federal authorities arrested two Lucent scientists and a third man described as their business partner on May 4, charging them with stealing source code for software associated with Lucent's PathStar Access Server and sharing it with Datang Telecom Technology Co., a Beijing firm majority-owned by the Chinese government. The software is considered a 'crown jewel' of the company. Chinese nationals Hai Lin and Kai Xu were regarded as 'distinguished members' of Lucent's staff up until their arrests. The motivation for the theft, according to court documents, was to build a networking powerhouse akin to the 'Cisco of China.' The men faced charges of conspiracy to commit wire fraud, punishable by a maximum five years in prison and a $250,000 fine." About a year later, in April 2002, NewsScan reported, the

[17] Anonymous (2001)
[18] *NewsScan* is no longer published. < http://www.newsscan.com >

accused were also charged with stealing secrets from four companies in addition to Lucent[:]…. Telenetworks, NetPlane Systems, Hughes Software Systems, and Ziatech." The two, working with Yong-Qing Cheng, were "thought to have developed a joint venture with the Datang Telecom Technology Company of Beijing to sell a clone of Lucent's Path Star data and voice transmission system to Internet providers in China." Kai Xu and Yong-Qing Cheng signed a plea agreement admitting guilt but Hai Lin fled prosecution.

- In April 2003, the United States Attorney's Office for the Northern District of California announced that a citizen of Singapore had pled guilty to theft of trade secrets. He admitted that in early 2002, while working for a language translation company, he delivered a laptop computer and a hard drive that contained trade secrets and confidential proprietary information to a competitor and asked for $3M in payment.[19]

- In July 2004, an Indian software engineer employed by a US company's software development center in India was accused of "zipping up" proprietary software source code for printing identification cards and uploading it to her personal e-mail account.[20]

- Two Chinese nationals, Fei Ye and Ming Zhong, pleaded guilty in December 2006 to charges of economic espionage on behalf of the People's Republic of China. They were arrested in November 2001 with stolen trade secrets in their luggage; the information was taken from Sun Microsystems and Transmeta Corporation. The agents were planning to design a competing microprocessor using the stolen designs; profits were to have been shared with the City of Hangzhou and the Province of Zhejiang. The agents' company was funded in part by the National High Technology Research and Development Program of China (aka the "863 Program").[21]

- Lan Lee (aka Lan Li), 42, of Palo Alto, and Yuefei Ge, 34, of San Jose, were indicted on September 26, 2007 in federal court for allegedly conspiring "to steal trade secrets from their employer at the time, NetLogics Microsystems, and from Taiwan Semiconductor Manufacturing Corporation, another company where they were not employed. The superseding indictment further alleges that the defendants created a company, SICO Microsystems, Inc., for the purpose of developing and marketing products derived from and using the stolen trade secrets. The trade secrets involved related to computer chip design and development. The defendants sought to obtain venture capital funding for their company from the government of China, in particular the 863 Program and the General Armaments Department."[22]

For extensive historical records of intelligence cases, see the *CI Reader* volumes from the Office of the National Counterintelligence Executive. At the time of writing (January 2008), there were four volumes available for download as PDF files.[23]

[19] Jacobs (2003)
[20] Ribeiro (2004)
[21] Macaulay (2006)
[22] LaBauve (2007)
[23] ONCIX (2001?)

China and Titan Rain

The immense growth and development of the Chinese economy, especially in the 1990s and 2000s, has been accompanied by a rising tide of industrial espionage and criminal hacking originating from the People's Republic of China (PRC). The *CIA Factbook* section on China's economy reports that since the shift away from a Soviet-style central-command economy, starting in 1978, the Chinese Gross Domestic Economy has quadrupled. "Measured on a purchasing power parity … basis, China in 2004 stood as the second-largest economy in the world after the US…." The real growth in Gross Domestic Product (GDP) is estimated at 9.1% in 2004, which accords with figures ranging from 8-12% in recent years (the US rate of increase of GDP was 4.4% in 2004).[24]

In summary, China is already a world power and will soon be a superpower challenging the United States and Europe at all levels of geopolitical competition.

TIME Magazine published an interesting report by Nathan Thornburgh on Aug 29, 2005 about an investigation code-named TITAN RAIN that began in late 2003. As an information systems security officer (ISSO) for Sandia National Laboratories of the US Department of Energy, Shawn Carpenter noticed a flood of expert hacker activity focusing on data theft from a wide range of "the country's most sensitive military bases, defense contractors and aerospace companies." Carpenter discovered that "the attacks emanated from just three Chinese routers that acted as the first connection point from a local network to the Internet." Carpenter worked with US Army and FBI investigators to learn more about the attacks and the attackers. According to Thornburgh, various analysts judge that "Titan Rain is thought to rank among the most pervasive cyberespionage threats that U.S. computer networks have ever faced."[25]

So was Carpenter treated as a hero by Sandia managers?

Well, no. He was fired for inappropriate and unauthorized use of Department of Energy computer resources and information. I'm sorry for Carpenter, but I have already written many times in this venue and elsewhere that it is a really bad idea to use corporate resources without written permission from appropriate authorities, especially if there is any risk of being perceived as a law-breaker. Even if Carpenter had acquired written support from his US Army and FBI handlers, that still might not have protected him against termination of employment. I cannot criticize Sandia managers on this count, and I understand that applying policy firmly is an important element of effective security management.

Incidentally, according to the *TIME* article, the government of the PRC denied any involvement in the hacker activity – but it also flatly refused to cooperate with US law enforcement authorities investigating the case.

[24] CIA (2007)
[25] Thornburgh (2005)

Blocking IP Traffic from Specific Nations

Scott Granneman wrote a thoughtful and stimulating commentary about Chinese hacker attacks in *The Register* on the 31st of August 2005.[26] He also mentioned the Titan Rain case but he focused first on the experience of some personal friends of his who run Web-hosting services.

They both independently discovered that their systems were being swamped by a flood of peculiar requests originating in a wide range of sites in the People's Republic of China (PRC). He wrote, "Both of my friends thought about their situations, and both came to the same conclusion: block the entire IP ranges! Use WHOIS to look up the IP address' range, then block 'em with the server's firewall. This quickly grew into a mammoth, seemingly neverending task, but it immediately began to pay off. Fishy web server requests tapered off greatly, and while there are still a few every day, it's now become a manageable problem. If things keep up at the same pace, sometime in the next few months they're going to have blocked every IP in China."

Granneman asked whether his friends had told their clients about their new policy of blocking all packets originating in the .CN domain; they said no.

Granneman, to his credit, raises two ethical questions:

1) Should his friends have told the clients about the global block on Chinese access to their Web sites?

2) Is there something wrong with blocking all access to a Web site for all users in a national domain?

For the first question, I think that simple ethical rules dictate that his friends should indeed have informed their clients of the new policy. One rule in ethical decision making is to consider all the stakeholders affected by a decision, and their clients are potentially affected. Another is that openness characterizes appropriate actions; a desire for secrecy always raises questions about whether a course of action is ethical (it doesn't mean that all secrecy is bad, just that it raises questions that should be answered).

However, for the second, I cannot conceive of how anyone could reasonably argue that the owners of a private Web site have any limits whatsoever on how they restrict access to their information. The Web is a method for voluntarily sharing documents (and now, much more) using standard protocols (http, html and so on). Nothing in the technology removes the absolute right of the data owner to control how that information is shared. For example, if a copyright holder chooses to restrict access to published documents by requiring registration, that's fine. If they require access controls using a userID and a password, that's fine. If they require users to buy smart cards and log in using one-time passwords, that's a real pain but it's also fine. If they require users to have biometric equipment for retinal scans, brain-wave measurements and a signature in blood giving away rights to the user's house, that may be crazy but it's also perfectly

[26] Granneman (2005)

legal. The worse the restrictions, the fewer the users, but no one has an absolute right to access any document on a privately-owned site on the Web.

So if a private Web-site owner wants to block all packets originating from the PRC, there is absolutely nothing morally or legally wrong with such a decision.

Personally, I have blocked all e-mail with country domains from which large amounts of spam originate; if someone in those countries wants to communicate with me, they can write me a letter. Immoral? No. Unethical? No.

MY e-mail. MY Web site. Don't bother me if I don't like you, your ISP or your country!

Works Cited

Anonymous (2001). "More theft of trade secrets." Article in *CIND* (*Counterintelligence News and Developments)* volume 2 (June 2001). No longer currently available online except in Web Archives (stability of link is indeterminate).
< http://web.archive.org/web/20050310140232/http://www.nacic.gov/archives/nacic/news/2001/jun01.html >

ASIS (2007). "Trends in Proprietary Information Loss Survey Report." PDF available at < http://www.asisonline.org/newsroom/surveys/spi2.pdf >

Bernstein, R. (2005). "Foreign-Born Population Tops 34 Million, Census Bureau Estimates." U.S. Census Bureau News
< http://www.census.gov/Press-Release/www/releases/archives/foreignborn_population/003969.html >

CIA – U.S. Central Intelligence Agency (2007). *The World Factbook.*
< https://www.cia.gov/library/publications/the-world-factbook/index.html > Downloads of current edition in various sizes of ZIP files available from
< https://www.cia.gov/library/publications/download/ >

Granneman, S. (2005). "On blocking Chinese IP addresses." *The Register* (31 Aug. 2005).
< http://www.theregister.co.uk/2005/08/31/blocking_chinese_ip_addresses/ >

Jacobs, M. J. (2003). "Chicago, Illinois Man Pleads Guilty to Theft of Trade Secrets, Offered to Sell Online Interpreter's Information." U.S. Department of Justice.
< http://www.usdoj.gov/criminal/cybercrime/sunPlea.htm >

Kabay (2007). Understanding studies and surveys of computer crime.
< http://www2.norwich.edu/mkabay/methodology/crime_stats_methods.htm > (HTML) or
< http://www2.norwich.edu/mkabay/methodology/crime_stats_methods.pdf > (PDF)

Kabay, M. E. (1994-2006). Information Security Year in Review Database. PDF reports and Access MDB files freely available from < http://www2.norwich.edu/mkabay/iyir >)

LaBauve, N. (2007). "Two Bay Area Men Indicted on Charges of Economic Espionage." U. S. Department of Justice.
< http://www.usdoj.gov/usao/can/press/2007/2007_09_26_lee.ge.indicted.press.html >

Macaulay, L. (2006). "Two Men Plead Guilty to Stealing Trade Secrets from Silicon Valley Companies to Benefit China: First Conviction in the Country for Foreign Economic Espionage." U.S. Department of Justice.
< http://www.usdoj.gov/criminal/cybercrime/yePlea.htm >

NACIC Report (1995)
< http://www.ncix.gov/publications/reports/fecie_all/FECIE_1995.pdf >

NACIC Report (2000)
< http://www.ncix.gov/publications/reports/fecie_all/fecie_2000.pdf >

ONCIX (2001?) *CI Reader: An American Revolution into the New Millennium*. Office of the National Counterintelligence Executive. [Author(s) unknown despite use of first person singular pronouns; date of publication unclear.]
< http://www.ncix.gov/issues/CI_Reader/index.html >

Ribeiro, J. (2004). "Source code stolen from U.S. software company in India: Jolly Technologies blamed an insider for the theft." *Computerworld.*
<
http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,95045,00.html
>

Spooner, J. G. (2005). "IBM-Lenovo deal said to get national security review." CNET News.com
< http://www.news.com/IBM-Lenovo-deal-said-to-get-national-security-review/2100-1003_3-5547546.html >

Thornburgh, N. (2005). "The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them)." *TIME Magazine* (Aug. 29, 2005).
< http://www.time.com/time/magazine/printout/0,8816,1098961,00.html >

U. S. Census Bureau (2005). MS-Excel file from
< http://www.census.gov/popest/states/asrh/tables/SC-EST2004-04.xls >

US Secretary of Defense (2007). Annual Report to Congress: Military Power of the People's Republic of China 2007.
< http://www.globalsecurity.org/military/library/report/2007/2007-prc-military-power.htm >
Chapter 5: Resources for Force Modernization
< http://www.globalsecurity.org/military/library/report/2007/2007-prc-military-power05.htm >