FBI TAMPA CI STRATEGIC PARTNERSHIP NEWSLETTER

June 1, 2011
Volume 3 Issue 6

Federal Bureau of Investigation
11000 Wilshire Boulevard, Suite 1700
Los Angeles, California 90024, 310.477.6565

INSIDE THIS ISSUE:

COUNTERINTELLIGENCE (CI) TRENDS

THE INSIDER THREAT; SAFEGUARDING TRADE SECRETS PROPRIETARY INFORMATION AND RESEARCH

THE INSIDER THREAT

The FBI has recently produced a new pamphlet (posted online at the web link below) discussing the risks associated with trusted "insiders" who take full advantage of their access to information to steal that information. This pamphlet is an excellent training tool. It discusses some of the indicators that individuals might be involved in illicit activity. It also discusses possible causative factors, and provides brief snippets from recent cases of "insiders" convicted of espionage, economic espionage or theft of trade secrets and proprietary information.

The pamphlet may be downloaded as a .pdf file from the below web link. If you are interested in receiving copies of this pamphlet in its original form, or are interested in receiving a Counterintelligence Vulnerability self-assessment tool, please contact one of the FBI Strategic Partnership Program persons named elsewhere in this newsletter.

http://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat

A company can often detect or control when an outsider (non-employee) tries to access company data either physically or electronically, and can mitigate the threat of an outsider stealing company property. However, the thief who is harder to detect and who could cause the most damage is the insider—the employee with legitimate access. That insider may steal solely for personal gain, or that insider may be a "spy"—someone who is stealing company information or products in order to benefit another organization or country.

The Insider Threat
An introduction to detecting and deterring an insider spy.

This brochure serves as an introduction for managers and security personnel on how to detect an insider threat and provides tips on how to safeguard your company's trade secrets.

Protect Your Intellectual Property

Theft of intellectual property is an increasing threat to organizations, and can go unnoticed for months or even years.

There are increased incidents of employees taking proprietary information when they believe they will be, or are, searching for a new job.

Congress has continually expanded and strengthened criminal laws for violations of intellectual property rights to protect innovation and ensure that egregious or persistent intellectual property violations do not merely become a standard cost of doing business.

A domestic or foreign business competitor or foreign government intent on illegally acquiring a company's proprietary information and trade secrets may wish to place a spy into a company in order to gain access to non-public information. Alternatively, they may try to recruit an existing employee to do the same thing.

Personal Factors

There are a variety of motives or personal situations that may increase the likelihood someone will spy against their employer:

Greed or Financial Need: A belief that money can fix anything. Excessive debt or overwhelming expenses.

Anger/Revenge: Disgruntlement to the point of wanting to retaliate against the organization.

Problems at work: A lack of recognition, disagreements with co-workers or managers, dissatisfaction with the job, a pending layoff.

Ideology/Identification: A desire to help the "underdog" or a particular cause.

Divided Loyalty: Allegiance to another person or company, or to a country besides the United States.

Adventure/Thrill: Want to add excitement to their life, intrigued by the clandestine activity, "James Bond Wannabe."

Vulnerability to blackmail: Extra-marital affairs, gambling, fraud.

Ego/Self-image: An "above the rules" attitude, or desire to repair wounds to their self-esteem. Vulnerability to flattery or the promise of a better job. Often coupled with Anger/Revenge or Adventure/Thrill.

Ingratiation: A desire to please or win the approval of someone who could benefit from insider information with the expectation of returned favors.

Compulsive and destructive behavior: Drug or alcohol abuse, or other addictive behaviors.

Family problems: Marital conflicts or separation from loved ones.

Organizational Factors

Organizational situations may increase the ease for thievery:

The availability and ease of acquiring proprietary, classified, or other protected materials. Providing access privileges to those who do not need it.

Proprietary or classified information is not labeled as such, or is incorrectly labeled.

The ease that someone may exit the facility (or network system) with proprietary, classified or other protected materials.

Undefined policies regarding working from home on projects of a sensitive or proprietary nature.

The perception that security is lax and the consequences for theft are minimal or non-existent.

Time pressure: Employees who are rushed may inadequately secure proprietary or protected materials, or not fully consider the consequences of their actions.

Employees are not trained on how to properly protect proprietary information.

Behavioral Indicators

Some behaviors may be a clue that an employee is spying and/or methodically stealing from the organization:

Without need or authorization, takes proprietary or other material home via documents, thumb drives, computer disks, or e-mail. Inappropriately seeks or obtains proprietary or classified information on subjects not related to their work duties.

Interest in matters outside the scope of their duties, particularly those of interest to foreign entities or business competitors.

Unnecessarily copies material, especially if it is proprietary or classified.

Remotely accesses the computer network while on vacation, sick leave, or at other odd times.

Disregards company computer policies on installing personal software or hardware, accessing restricted websites, conducting unauthorized searches, or downloading confidential information.

Works odd hours without authorization; notable enthusiasm for overtime work, weekend work, or unusual schedules when clandestine activities could be more easily conducted.

Unreported foreign contacts (particularly with foreign government officials or intelligence officials) or unreported overseas travel.

Short trips to foreign countries for unexplained or strange reasons. Unexplained affluence; buys things that they cannot afford on their household income.

Engages in suspicious personal contacts, such as with competitors, business partners or other unauthorized individuals.

Overwhelmed by life crises or career disappointments.

Shows unusual interest in the personal lives of co-workers; asks inappropriate questions regarding finances or relationships.

Concern that they are being investigated; leave straps to detect searches of their work area or home; searches for listening devices or cameras.

Many people experience or exhibit some or all of the above to varying degrees; however, most people will not cross the line and commit a crime.

You Can Make A Difference

Organizations need to do their part to deter intellectual property theft:

- Educate and regularly train employees on security or other protocols.
- Ensure that proprietary information is adequately, if not robustly, protected.
- Use appropriate screening processes to select new employees.
- Provide non-threatening, convenient ways for employees to report suspicions.
- Routinely monitor computer networks for suspicious activity.
- Ensure security (to include computer network security) personnel have the tools they need.

Remind employees that reporting security concerns is vital to protecting your company's intellectual property, its reputation, its financial well-being, and its future. They are protecting their own jobs. Remind them that if they see something, to say something.

Get Assistance

Being aware of potential issues, exercising good judgment, and conducting discrete inquiries will help you ascertain if there is a spy in your midst. However, if you believe one of your employees is a spy or is stealing company trade secrets, do not alert the person to the fact that he/she is under suspicion, but seek assistance from trained counterintelligence experts–such as the FBI. The FBI has the tools and experience to identify and mitigate such threats. If asked to investigate, the FBI will minimize the disruption to your business, and safeguard your privacy and your data. Where necessary, the FBI will seek protective orders to preserve trade secrets and business confidentiality. The FBI is committed to maintaining the confidentiality and competitive position of US companies. The FBI will also provide security and counterintelligence training or awareness seminars for you and your employees upon request.

Recent Insider Theft Cases

Michael Mitchell, a sales clerk and engineer, became disgruntled and was fired from his job based on poor performance. Mitchell signed statements affirming he had returned all proprietary information to his employer and was reminded of nondisclosure policies. However, Mitchell kept numerous computer files, entered into a consulting agreement with a rival Korean company, and provided trade secrets from his former employer to that company. In March 2010, he was sentenced to 18 months in prison and ordered to pay his previous employer over $187,000.

Shalin Jhaveri, a technical operations associate, gave trade secrets to a person he believed was an investor willing to finance a business venture in India, and confirmed to the investor that the information he had taken from his employer was everything he needed to start the business. He confessed that he disguised his actions to evade detection. In January 2011, he was sentenced to time served (one year and fifteen days), three years probation, a $5,000 fine, and a $100 Special Assessment.

David Yen Lee accepted a job on 27 February 2009 from a business competitor in China, but did not resign from his current employer until 16 March 2009. Lee admitted to downloading trade secrets from his employer's secured computer system for several months prior to his resignation. The stolen trade secrets were worth between $7 million and $20 million. In December 2010, Lee was sentenced to 15 months in prison and three years supervised release.

Sergey Aleynikov, a computer programmer, worked for a company on Wall Street from May 2007 until June 2009. During his last few days at that company, he downloaded, and transferred 32 megabytes of proprietary computer codes– a theft that could have cost his employer millions of dollars. He hoped to use the computer codes at his new Chicago-based employer. He attempted to hide his activities, but the company discovered irregularities through its routine network monitoring systems. In December 2010, Aleynikov was found guilty of theft of trade secrets and transportation of stolen property in foreign commerce.

Greg Chung spied for China from 1979-2006. Federal charges against Chung consisted of stealing trade secrets about the space shuttle, the Delta IV rocket and the C-17 military cargo jet for the benefit of the Chinese government. Chung's motive was to "contribute to the Motherland." He was an engineer that stole hundreds of thousands of documents. He traveled to China under the guise of giving lectures while secretly meeting with Chinese government officials and agents. He was also encouraged to use Chi Mak (see below) to transfer information back to China. Chung was arrested in February 2008 and in February 2010 he was sentenced to over 15 years in prison.

Chi Mak admitted that he was sent to the United States in 1978 in order to obtain employment in the defense industry with the goal of stealing US defense secrets, which he did for 20 plus years. He most recently passed information on quiet electric propulsion systems for the next generation of US submarines, details on the Aegis radar system, and information on stealth ships being developed by the US Navy. The Chinese government tasked Mak to acquire information on other specific technologies. Mak recruited family members to encrypt and covertly courier information back to China. In May 2007, Chi Mak was convicted of conspiracy, attempting to violate export control laws, failing to register as an agent of a foreign government, and making false statements to investigators. He was sentenced to over 24 years in prison, and four members of his family received varying sentences of up to 10 years in prison.

For additional information, training, or assistance, contact the FBI.

SAFEGUARDING TRADE SECRETS PROPRIETARY INFORMATION AND RESEARCH

The FBI has recently produced a new pamphlet (posted online at the web link below) providing some tips and guidance for the protection of intellectual property. The pamphlet may be downloaded as a .pdf file from the below web link. If you are interested in receiving copies of this pamphlet in its original form, or are interested in receiving the vulnerability self-assessment tool discussed near the end of the pamphlet, please contact one of the FBI Strategic Partnership Program persons named elsewhere in this newsletter.

Intellectual Property Protection

http://www.fbi.gov/about-us/investigate/counterintelligence/intellectual-property-protection

Safeguard Your Company's Trade Secrets, Proprietary Information and Research

Domestic and foreign companies may try to illegally acquire your company's information. Foreign nations that seek to improve their economies and militaries target US technology companies.

Protect the programs and systems that support what makes your company successful and unique. If your company has a technological edge, expect your technology, and those with access to it, to be targeted. If your company has developed a process to manufacture an item at less cost than others, that manufacturing process may be targeted. If your company is negotiating with another company or country, the negotiators and negotiation strategy may be targeted. If your company has invested time and resources developing a product or idea—Protect It!

Common Tactics

■Computer hacking! (Electronic-device hacking)
■A visitor connects an electronic device to your system, such as a thumb drive, that adds malware or downloads your information
■Someone hacks into your network via a spear phishing attack
■An unattended laptop is accessed or stolen
■On-site visits to your company:
■Unauthorized photography or computer access. Unauthorized entry into restricted areas
■Asking questions outside the scope of the visit Review of publicly available sources
■Review of publicly available sources. Are you sharing too much information?
■Obtains your surplus equipment. Thousands of pages of stored information may still reside in the memory of a copier, printer, fax machine, etc
■Employment solicitation (try to hire your key employees)
■Theft or unauthorized photography of products at trade shows
■Burglary (including copying of restricted documents where the originals stay in-house)
■Dumpster diving – finding information in your company's trash

■Joint ventures
■Front companies
■Unsolicited requests for information
■Elicitation – developing a friendship with an employee with the intention of obtaining restricted data or products. The employee will see someone who appears non-threatening and interested in his/her work
■Electronic surveillance (listening devices in your hotel room, cell-phone hacking, etc.)

Theft of Intellectual Property Could Result in:

■Lost revenue
■Lost employment
■Damaged reputation
■Health and safety concerns from counterfeit products
■Lost investment for research (R&D)
■Delays or interruption in production

Who Might Steal Your Intellectual Property?

■Domestic and foreign commercial rivals
■Domestic and foreign start-up companies
■Foreign intelligence officers (spies)
■Disgruntled employees
■Opportunists (lone wolves)
■Organized criminals

Insider Threats
Look for warning signs that an employee may be gathering and passing information outside your company.

Foreign Travel
When traveling to a foreign country, you and your company's information are at greater risk.

■Many foreign countries do not have legal restrictions against technical surveillance
■Some foreign governments help their domestic corporations collect competitive intelligence

Protection Strategies

Assess your company's information security vulnerabilities and fix or mitigate the risks associated with those vulnerabilities.

Do not store private information vital to your company on any device that connects to the Internet.

Use up-to-date software security tools. Many firewalls stop incoming threats, but do not restrict outbound data. Competitive intelligence hackers try to retrieve data stored on your network.
Educate employees on spear phishing email tactics. Establish protocols for quarantining suspicious email.

Ensure your employees are aware of and are trained to avoid unintended disclosures.

Remind employees of security policies on a regular basis through active training and seminars. Use signs and computer banners to reinforce security policies. Document employee education and all other measures you take to protect your intellectual property.

Ensure human resource policies are in place that specifically enhance security and company policies. Create clear incentives for adhering to company security policies.

Ask the FBI or other security professionals to provide additional awareness training.

The FBI can provide a vulnerability self-assessment tool.

Contact Law Enforcement
You are ultimately responsible for protecting your own intellectual property. Congress has continually expanded and strengthened criminal laws for violations of intellectual property rights to protect innovation; however, you need to take reasonable steps to protect your intellectual property and products, and document those measures.

Violations that may apply: Economic Espionage, Theft of Trade Secrets, Mail Fraud, Wire Fraud, Interstate Transportation of Stolen Property, Export Control, and Intellectual Property Rights.

If you believe your company is a victim of these crimes, contact the FBI or the National Intellectual Property Rights Coordination Center. Investigators cannot act if they are not aware of the problem. The FBI will minimize the disruption to your business, and safeguard your privacy and your data during its investigation. Where necessary, the FBI will seek protective orders to preserve trade secrets and business confidentiality.

Safeguard Your Company's Trade Secrets, Proprietary Information and Research.

www.fbi.gov
www.ice.gov/iprcenter

ARRESTS, TRIALS AND CONVICTIONS

China's spying seeks secret US info

http://www.deseretnews.com/mobile/article/700133408/AP-IMPACT-Chinas-spying-seeks-secret-US-info.html

By Pauline Arrillaga

Associated Press

Published: Saturday, May 7, 2011 10:01 a.m. MDT

ALEXANDRIA, Va. — The young man stood before the judge, his usually neatly trimmed hair now long enough to brush the collar of his prison jumpsuit. Glenn Duffie Shriver had confessed his transgressions and was here, in a federal courtroom with his mother watching, to receive his sentence and to try, somehow, to explain it all.

When the time came for him to address the court, he spoke of the many dreams he'd had to serve his country.

"Mine was to be a life of service," he said. "I could have been very valuable. That was originally my plan."

EDITOR'S NOTE — China, ever more powerful, has become a major instigator of espionage in the United States. First of a two-part series on Beijing's efforts, many successful, to steal American secrets and technology.

He had been a seemingly all-American, clean-cut guy: No criminal record. A job teaching English overseas. In letters to the judge, loved ones described the 29-year-old Midwesterner as honest and caring — a good citizen. His fiancée called him "Mr. Patriot."

Such descriptions make the one that culminated in the courtroom all the more baffling: Glenn Shriver was also a spy recruit for China. He took $70,000 from

individuals he knew to be Chinese intelligence officers to try to land a job with a U.S. government agency — first the State Department and later the CIA.

And Shriver is just one of at least 57 defendants in federal prosecutions since 2008 charging espionage conspiracies with China or efforts to pass classified information, sensitive technology or trade secrets to intelligence operatives, state-sponsored entities, private individuals or businesses in China, according to an Associated Press review of U.S. Justice Department cases. Of those, nine are awaiting trial, and two are considered fugitives. The other defendants have been convicted, though some are yet to be sentenced.

Most of these prosecutions have received little public attention — especially compared with the headline splash that followed last summer's arrest of 10 Russian "sleeper agents" who'd been living in suburban America for more than a decade but, according to Attorney General Eric Holder, passed no secrets.

Contrast that with this snapshot:

—In Honolulu, a former B-2 bomber engineer gets 32 years in prison for working with the Chinese to develop a vital part for a cruise missile in a case that a high-ranking Justice Department official said resulted in the leak of "some of our country's most sensitive weapons-related designs."

—In Boston, a Harvard-educated businessman is sent to prison, along with his ex-wife, for conspiring for a decade to illegally export parts used in military radar and electronic warfare systems to research institutes that manufacture items for the Chinese military. The Department of Defense concluded the illegal exports "represented a serious threat to U.S. national and regional defense security interests."

—In Los Angeles, a man goes to jail for selling Raytheon-manufactured thermal imaging cameras to a buyer in Shanghai whose company develops infrared technology. The cameras are supposed to be restricted for export to China because of "their potential use in a wide variety of military and civilian applications," according to court documents.

—And in Alexandra, Va., there is Shriver, who told the judge quite simply: "Somewhere along the way, I climbed into bed with the wrong people."

All five of these defendants were sentenced over just an 11-day span earlier this year.

In Shriver's case, when once he asked his Chinese handlers — "What, exactly, do you guys want?" — the response, as detailed in court documents, was

straightforward: "If it's possible, we want you to get us some secrets or classified information."

Despite denials from Beijing, counterintelligence experts say the cases reveal the Chinese as among the most active espionage offenders in America today, paying more money and going to greater lengths to glean whatever information they can from the United States.

For years, U.S. counterintelligence experts have cited a growing espionage threat from China, the product of an ever-more competitive world in which technology is as vital as political intelligence — but a sign, too, of China's increasing prosperity, persistence and patience.

Recent cases reveal not only a high level of activity but also signs of changing tactics and emboldened efforts. In one case, a convicted spy managed to convince not one but two U.S. government officials to pass him secret information, telling them it was going to Taiwan when he instead passed it to a Chinese official.

The recruitment of more non-Chinese, such as Shriver, also represents a shift, said Larry Wortzel, who serves on the U.S.-China Economic and Security Review Commission.

And then there are the so-called "espionage entrepreneurs," motivated simply by money.

When asked about the recent cases, the Chinese Foreign Ministry questioned the statistics, responding in a statement: "To speak of the Chinese side's so-called 'espionage activities' in the United States is pure nonsense with ulterior motives." However, Joel Brenner, who served as the U.S. National Counterintelligence Executive from 2006 to 2009, said: "The Chinese espionage threat has been relentless recently ... we've never seen anything like it. Some of its public. Some of its private. And some of it lies in that ambiguous area in between."

Today's "agents" are professors and engineers, businessmen exporting legitimate products while also shipping restricted technology and munitions, criminal capitalists who see only dollar signs. While some may be acting at the direction of a government handler, others supply information to firms for either private enterprise or state-sponsored research — or both.

Driving all of this, U.S. officials said, are China's desire to develop a modernized military and its burgeoning wealth; last year China surpassed Japan as the world's second-largest economy, behind only the United States.

"They have more money to pay for things," said Steve Pelak, a deputy chief of the Justice Department's counterespionage section who points to the amounts given to Shriver before he was ever in a position to access, much less pass, secrets.

Still more money is going to private firms to help develop and build China's military technology, sometimes through parts obtained illegally from U.S. manufacturers.

Indeed most of the Justice Department cases reviewed by the AP involve the illegal export of restricted defense-related parts or so-called "dual-use" technology, which can have commercial or military applications. These are items such as integrated circuits for radar systems, high-power amplifiers designed for use in early-warning radar and missile target acquisition systems, and military grade night-vision technology.

But that only scratches the surface. Other cases involve the theft of trade secrets by individuals once employed at major U.S. corporations, including Boeing, Motorola and Dow. In some instances, the secrets were computer source codes or, in cases still awaiting trial, related to the development of organic pesticides and telephone communications technology.

Stolen information about the space shuttle and technical data about the capabilities of the U.S. Navy's nuclear-powered submarines have also been passed along.

While export cases and economic espionage comprise most of the China-related intelligence prosecutions in recent years, there have been a few notable instances of traditional espionage — among them the Shriver case and that of Tai Shen Kuo, a Louisiana businessman who obtained information from two federal government employees that he passed to China.

It all fits into what some experts call China's "vacuum cleaner" approach to information-collection: Catch whatever you can.

"It's a little like ... the cancer that you don't know your body has," said Michelle Van Cleave, another former National Counterintelligence Executive. "You don't know that you're in trouble until it manifests itself in ways that really, really hurt you."

"If you have customers in mainland China, please let us know if we could be of any help. In China, it seems impossible for most companies to buy directly from US. We can act as middleman for you."

It was 1996 and Zhen Zhou "Alex" Wu, a one-time schoolteacher in his native China who later studied at Harvard, was e-mailing a pitch for his business: A company dedicated to selling electronics components to Chinese customers. Based in Shenzhen, China, the company, Chitron, opened a single U.S. office in Waltham, Mass., to acquire desired technology.

The Massachusetts firm, federal authorities now say, was merely a front to facilitate the export of defense technology from U.S. manufacturers to Chinese military-related institutes. And Wu now sits in a federal prison after being sentenced in January to eight years for conspiring to illegally export restricted technologies.

According to the Department of Defense, the exported items are "vital for Chinese military electronic warfare, military radar, fire control, military guidance and control equipment, and satellite communications." Also included: parts "that the People's Liberation Army actively seeks to acquire."

The use of front companies, or private firms that may also do legitimate business, is a common way that China seeks information, said Pelak, who in 2007 was appointed the Justice Department's first national export control coordinator, focusing on illegal export of munitions and sensitive technology. Prosecutions have since gone up, and today two-thirds of federal illegal export cases involve either China or Iran.

Take the case of William Chi-Wai Tsu, an electrical engineer serving a three-year prison sentence for illegally shipping several hundred thumbnail-size integrated circuits to a Beijing company called Dimagit Science & Technology. Investigators said the circuits have a variety of applications, including use in sophisticated communications and military radar systems.

Among Dimagit's clients: a research institute affiliated with the state-owned China Aerospace Science and Technology Corp. Dimagit's catalog, according to court records, promised: "We unswervingly take providing the motherland with ... electronic technical support to revitalize the national defense industry as our mission."

Court records describe how Tsu went about acquiring restricted parts: He created a fictitious company and used the California address of a friend for shipping. He then provided false end-user statements to American electronics distributors, promising that the parts he sought were not for export but for domestic use — specifically a project with Cisco Systems. If a distributor pressed Tsu, he would claim that nondisclosure agreements prevented him from providing more detail.

Similar tactics were used in a case still awaiting sentencing in Seattle. Lian Yang, a former software engineer at Microsoft, pleaded guilty in late March to attempting to buy restricted technology for a "partner" in China — specifically 300 radiation-hardened programmable semiconductor devices that are used in satellites. In conversations with a confidential FBI source, Yang suggested creating a fake U.S. company to list as the end-user.

Yang was arrested last Dec. 3 after he handed $20,000 to undercover agents in exchange for five of the devices. His sentencing is set for June 30. Prosecutors argued in court papers that the offense "amounted to a form of espionage on behalf of" China.

However, some defense attorneys counter that these export cases aren't espionage at all or even deliberate attempts to circumvent U.S. laws — but rather an outgrowth of confusing policies and, perhaps, overzealous prosecutors. In the Chitron case, appeals lawyers for Alex Wu insist U.S. export regulations don't make clear enough what can and cannot be legally exported.

"Wu and others at his firm were not equipped and did not have the training needed to understand this country's extremely complicated export control laws," said his lawyer, Michael Schneider.

Stephanie Siegmann, the assistant U.S. attorney who prosecuted the case, responded that evidence clearly showed that Wu did understand the restrictions. One spreadsheet found on his computer was titled, "GP (Gross Profit) for USA Restricted Military Parts." Among the parts exported: phase shifters used in military radar systems.

"With such equipment," the Department of Defense's Defense Technology Security Administration concluded, "China could defeat U.S. weapon systems." Earlier this year, retired FBI agent I.C. Smith gave a speech called "China's Mole" at the International Spy Museum in Washington, D.C. It was about a man who landed a job with the Central Intelligence Agency and later turned out to be a spy for China.

He was referring to one of the most damaging Chinese espionage cases of all time: the infiltration of Larry Chin, who in 1986 admitted to spying for China during his almost three decades with the CIA. As a former Chinese counterintelligence supervisor, Smith helped investigate Chin, and he was stunned to learn of the 5½-year recruitment of Glenn Shriver and China's "run at the front door" of America's pre-eminent intelligence agency.

"The Chinese," Smith said, "still have the capacity to surprise."

How did they do it in Shriver's case? Standing before a federal judge on a blustery day in January, Shriver tried to explain how he went down the path to betrayal.

"It started out fairly innocuous," he recalled. During a college study-abroad program in Shanghai, he was taken with Chinese culture and became proficient in Mandarin. After graduating from Grand Valley State University in Michigan in 2004, he returned to China to look for work.

Shriver was just 22 years old when, in October 2004, he first met a woman in Shanghai called "Amanda." According to court documents, he'd responded to an English-language ad looking for scholars of East Asian studies to write political papers. He wrote one about U.S.-China relations regarding North Korea and Taiwan, and was paid $120.

"Amanda" later asked Shriver if he'd be interested in meeting some other people — two men he came to know as "Mr. Wu" and "Mr. Tang."

As outlined in court documents and Shriver's own statements, their conversations, at first, focused on developing a "friendship." The men asked Shriver what type of work he was interested in and said that if he planned on seeking a job with a U.S. government agency, "we can be close friends." Had he ever thought about working for the U.S. State Department or, perhaps, the CIA?

"That would be pretty good," they told him.

"Only one time was I told that they would like secrets," Shriver told the judge.

Six months after first meeting "Amanda," Shriver applied for a job with the U.S. State Department. Though he failed the foreign service exam, the intelligence officers paid him $10,000. A year later, in April 2006, he took the exam a second time but again failed. He was nevertheless paid $20,000.

Then, in June 2007, Shriver applied for a position in the clandestine branch of the CIA. A few months later, he asked the Chinese intelligence officers for $40,000 for his efforts.

During all this time, friends and family — Shriver's mother, especially — thought he was just trying to figure out what to do with his life. He talked about becoming a police officer or joining the Peace Corps. Eventually he returned overseas, this time to Korea, where he taught English and got engaged.
No one knew he was continuing to communicate with his Chinese handler, "Amanda."

In June 2010, Shriver underwent a series of final security screening interviews at the CIA in Virginia. A week later, he was arrested — U.S. officials wouldn't disclose what led them to him — and his clandestine life unraveled.

"Nobody knew. Nobody," said his mother, Karen Chavez. "He was a good kid. ... I don't know what he was thinking."

The closest her son came to an explanation was when he told the sentencing judge: "I think I was motivated by greed."

In a telephone interview from prison in April, Shriver tried to expand on that. "When you're 23 years old living in a very fun city, you almost get addicted to money ...," he told the AP. "After a while it's kind of like: OK, I'm kind of up on what these guys are doing. But by then it's just money getting thrown at you. I'm just like ... I can apply to this, get some money and then just continue on with my life."

Shriver pleaded guilty to conspiracy to communicate national defense information and is serving a four-year prison term.

It's true that he was, after all, never in a position to actually do any spying. No harm done? That may depend on how you look at it.

"This case shows an aggressive attempt by (China) to recruit an American citizen and attempt to place him in one of the nation's premier intelligence agencies," said Neil MacBride, the U.S. attorney for the Eastern District of Virginia, whose office has handled a number of China-related intelligence cases.

"Foreign intelligence services are watching," he said, "and they're looking for any weakness they can identify and exploit."

Pauline Arrillaga, a Phoenix-based national writer for The Associated Press, can be reached at features (at) ap.org.

Sailor pleads guilty to espionage charges in Norfolk

http://hamptonroads.com/print/600481

NORFOLK

A Navy intelligence specialist admitted Thursday that he smuggled classified documents out of Fort Bragg in folders and his pants pockets, then sold them for $11,500 to a man he believed was a Chinese agent.

Petty Officer 2nd Class Bryan Minkyu Martin, 22, pleaded guilty Thursday to four counts of attempted espionage and seven counts of mishandling classified information.

He had faced 15 charges and the possibility of life in prison. In exchange for his guilty pleas, the remaining charges will be dropped and he will receive a reduced sentence.

A reservist, Martin was arrested in December in North Carolina. At the time he was at Joint Special Operations Command at Fort Bragg training to deploy to Afghanistan, although he was assigned to the Expeditionary Combat Readiness Center at Joint Expeditionary Base Little Creek in Virginia Beach.

Thursday marked the first day of his court-martial at Norfolk Naval Station. The proceedings began with Martin's guilty pleas and continued with several hours of discussion in which the military judge who will sentence him, Capt. Moira Modzelewski, made sure he understood the accusations and the ramifications of his pleas.

In the course of doing so, Modzelewski detailed Martin's crimes:

Over four meetings between Nov. 15 and Dec. 1, he passed more than a dozen secret and top secret documents and images to a man he believed to be a Chinese intelligence officer, who he knew only as "Mr. Lee."
In exchange, the Chinese officer - actually an undercover FBI agent - paid Martin a total of $11,500. After at least two of the transactions, Martin signed receipts for the payments.

Asked to describe the documents, Martin said they contained information about current naval operations and intelligence assessments, including photos, satellite images and details about U.S. operations in Afghanistan and Iraq.

Martin said he met Mr. Lee at three separate hotels in Spring Lake, N.C., near Fort Bragg. When they spoke by phone before their first meeting, Mr. Lee told Martin to look for the man reading a Chinese newspaper.

Martin said that at one point before their first meeting he became concerned that Mr. Lee wasn't who he said he was. He considered traveling to Beijing to verify Mr. Lee's identity but changed his mind.

He said he obtained the classified materials by downloading and printing them at his work station at Joint Special Operations Command.

Asked whether he believed the information would be passed to the Chinese government and used to its advantage, Martin said yes. "I knew my actions would harm the national security of the United States," he told Modzelewski, adding that he chose the Chinese because he believed they would pay him the most money.

He was arrested immediately after his fourth meeting with Mr. Lee. He said it wasn't until several days later that he learned Mr. Lee was really an FBI agent. Authorities have said they don't believe Martin actually delivered classified information to anyone not authorized to see it, although the government seems interested in investigating further: As part of Martin's pre-trial agreement, he promised in exchange for partial immunity to submit to as many interviews and polygraph tests as authorities want over the next two years.

Thursday's proceedings did not reveal why the FBI began looking into Martin or how he and Mr. Lee became connected.

Wearing dress whites and glasses, Martin was calm and cooperative in court. The sentencing phase of Martin's court martial is expected to finish today. Prosecutors plan to play three hours of surveillance video. Martin's parents and a psychologist are expected to testify on his behalf.

Martin enlisted in the Navy in 2006 and received a top-secret-level security clearance the following year. Before reporting to Fort Bragg last September, he was stationed at military facilities in Syracuse, N.Y.; Jackson, S.C.; San Diego; and Washington.

Navy records list his hometown as Mexico, N.Y.

He is being held at the Norfolk Naval Station brig.

Corinne Reilly, (757) 446-2949, corinne.reilly@pilotonline.com

Former L-3 Worker Indicted For Data Breach

http://www.aviationweek.com/aw/generic/story.jsp?id=news/awx/2011/04/07/awx_04_07_2011_p0-307312.xml&headline=Former%20L-3%20Worker%20Indicted%20For%20Data%20Breach&channel=defense

Apr 7, 2011

By Jeremy Pelofsky/Reuters

WASHINGTON

A Chinese national who previously worked at an L-3 Communications unit was indicted on Wednesday on charges he illegally took sensitive military technology to China, the U.S. Justice Department said.

Sixing "Steve" Liu, 47, was charged with one count of exporting U.S. defense information without a license and two counts of making false statements to U.S. authorities, according to the indictment by a federal grand jury in Newark, New Jersey.

He had previously been charged by criminal complaint, but the company was not identified. Liu has been detained pending a hearing later this week and his lawyer, James Tunick, declined to comment on the indictment.

Liu worked for L-3's Space & Navigation unit in New Jersey from March 2009 until Nov. 30, 2010 as an engineer on a precision navigation device.

On his return from a trip to Shanghai last November, U.S. Customs and Border Protection agents inspected Liu's laptop and discovered hundreds of documents that belonged to the company involving several technology programs, the indictment said.

Some of the material found on his computer included technical data related to defense items that are restricted from export without a license and Liu did not have one, according to the indictment.

During his two-week trip to Shanghai last year, he presented information at a technology conference, but the indictment said L-3 had not given Liu permission to present information to outsiders.

He was also charged with two counts of lying to U.S. Immigration and Customs Enforcement agents when they interviewed him about possible violations of export control laws.

The company said in a statement that it has "supported this investigation from the beginning and will continue to cooperate fully with federal authorities."

THREE INDIVIDUALS AND TWO COMPANIES INDICTED FOR CONSPIRING TO EXPORT MILLIONS OF DOLLARS WORTH OF COMPUTER-RELATED EQUIPMENT TO IRAN

http://www.bis.doc.gov/news/2011/doj04212011.htm

WASHINGTON - One individual and his company in New York and two others and their company in California were indicted today in the District of Columbia on charges of illegally exporting millions of dollars worth of computer-related equipment from the United States to Iran via the United Arab Emirates (UAE). The two indictments were announced by Todd Hinnen, Acting Assistant Attorney General for National Security; Ronald C. Machen Jr., U.S. Attorney for the District of Columbia; John Morton, Director of U.S. Immigration and Customs Enforcement (ICE); and David W. Mills, Assistant Secretary of Export Enforcement, U.S. Department of Commerce.

Jeng "Jay" Shih, 53, a U.S. citizen, and his Queens, N.Y. company, Sunrise Technologies and Trading Company, were indicted in the District of Columbia on 27 counts relating to the illegal export of computer-related equipment to Iran without first having obtained the required license from the Department of Treasury. The indictment charges Shih and his company with one count of conspiracy; 13 counts of violating the International Emergency Economic Powers Act (IEEPA); 13 counts of making or causing to be made false statements to the United States; and one allegation for criminal forfeiture of property and proceeds derived from these offenses. Shih was arrested on a criminal complaint in New York on April 6, 2011, and had his initial appearance in court in New York on April 7, 2011. If convicted, he faces a maximum sentence of 20 years in prison and a $1 million fine for each of the IEEPA counts and five years for each false statement count.

Massoud Habibion, 48, aka "Matt Habibion" and "Matt Habi," and Mohsen Motamedian, 43, aka "Max Motamedian" and "Max Ehsan," both U.S. citizens, and their Costa Mesa, Calif., company, Online Micro LLC, were indicted in the District of Columbia on 32 counts relating to the illegal export of computer-related equipment to Iran without the required license from the Department of Treasury. Habibion was charged with one count of conspiracy, 14 counts of violating IEEPA, 14 counts of making or causing false statements to the United States and four counts of obstruction of justice. Motamedian was charged with one count of conspiracy, 14 counts of violating IEEPA, 14 counts of making or causing false statements to the United States and one count of obstruction of justice. Habibion and Motamedian were arrested on a criminal complaint in California on April 7, 2011, and had their initial appearance in court in the Central District of California on April 7, 2011. If convicted, both defendants face a maximum sentence of 20 years in prison and $1 million fine for each of the IEEPA counts, and five years for each false statement and 20 years for each obstruction of justice count.

According to the affidavit filed in support of the Shih criminal complaint, in 2006, Commerce Department agents conducted an outreach visit to Shih's business in New York where they met Shih and informed him about U.S. laws governing the

export of goods from the United States to other countries, particularly embargoed countries like Iran. In April 2010, ICE-Homeland Security Investigations (HSI) agents seized hundreds of laptop computers that originated from Sunrise and were destined for Dubai, UAE. Communications related to these shipments indicated that the purchasers were located in Iran, according to the affidavit.

The affidavit alleges that agents subsequently identified a company in Dubai that was purchasing millions of dollars of computers from U.S. companies for export to Iran, through Dubai. ICE-HSI agents arrested one of the company's agents, who pleaded guilty in December 2010 and began cooperating with the government. In interviews with agents, this individual indicated that he and his company in Dubai had purchased millions worth of laptops from Shih in recent years for shipment to Iran, averaging $700,000 worth of computers each month. The affidavit alleges that agents also obtained documents indicating that more than 1,000 computers had been shipped by Shih's company to Dubai and later to Iran, between April 9, 2010, and May 28, 2010, alone.

In February 2011, the cooperating individual met with Shih in New York. In recorded conversations, Shih allegedly told the individual he was aware of the U.S. embargo against Iran and U.S. export control laws. According to the affidavit, Shih also told the cooperating individual how to avoid detection when shipping goods to Iran by using fake invoices and indicated that he treated the seizure of some of his shipments as a "loss" when reporting business income and loses on his U.S. taxes.

The affidavit filed in support of the complaint against Habibion and Motamedian alleges that a company in Dubai, referenced above, purchased millions of dollars worth of laptop computers from Online Micro and that these computers were subsequently shipped to Iran. According to the affidavit, the agent for the Dubai company, who was arrested, pleaded guilty and began cooperating with the government, told federal agents that Habibion and Motamedian sold roughly $300,000 worth of computers to the Dubai company each month and that Habibion and Motamedian fully understood that the computers were destined for Iran.

In December 2010, the cooperating individual met with Habibion and Motamedian, wherein these defendants allegedly instructed the cooperating individual to make fake invoices to conceal that Iran was the destination of the shipments and to indicate that the end-users were in Dubai. In addition, the affidavit alleges that in a Jan. 5, 2011, meeting, Habibion told the cooperating individual to lie to federal agents about conducting business in Iran, stating, "If they ask you, for instance, 'Do you do business in Tehran?' 'No, I don't have any

business in Tehran. I go there to visit my family, but I have no business there.' They will ask such questions; it is part of their routine."

This investigation is being conducted by the ICE-HSI field offices in San Diego and New York and the Department of Commerce Office of Export Enforcement field offices in New York and Los Angeles, with assistance from ICE-HSI offices in Chicago, Newark, N.J., Los Angeles and Orange County, Calif. The Department of Homeland Security's U.S. Customs and Border Protection also assisted in the investigation.

The prosecution is being handled by Assistant U.S. Attorneys Anthony Asuncion and T. Patrick Martin, from the U.S. Attorney's Office for the District of Columbia, and Trial Attorney Jonathan C. Poling from the Counterespionage Section of the Justice Department's National Security Division. The U.S. Attorney's Offices for the Central District of California and Eastern District of New York also provided assistance.

The public is reminded that an indictment and criminal complaint contain mere allegations and that defendants are presumed innocent unless and until proven guilty.

Broomfield man charged with giving defense data to South Korea

http://www.broomfieldenterprise.com/ci_17924387

By Enterprise staff

Posted: 04/25/2011 02:34:08 PM MDT

A Broomfield man was charged last week with providing technical defense data to South Korea.

Young Su Kim, 43, pleaded not guilty on Thursday and was released on a personal recognizance bond, according to a news release from U.S. Attorney's Office in Denver.

The data in question is related to a Lens No. 3 RTS and a Prism/Lens No. 3 assembly, according to the news release. The data is on the U.S. Munitions List, which is regulated by the U.S. State Department. Kim did not have the necessary license or written permission to share the information, according to the news release.

If convicted, Kim could face up to 10 years in prison and a fine of up to $1 million.

Upon conviction, the government also is seeking any proceeds from the data transfer or a judgment of $36,000.

The case was investigated by the U.S. Immigration and Customs Enforcement Homeland Security Investigations and the Defense Criminal Investigative Service.

California man gets 25 years for missile-smuggling plot

http://www.sacbee.com/2011/05/09/3613653/calif-man-gets-25-years-for-missile.html

The Associated Press

Published Monday, May. 09, 2011

LOS ANGELES -- The first person indicted under a federal anti-terrorism law adopted after the Sept. 11 attacks was sentenced Monday to 25 years in prison for attempting to smuggle anti-aircraft missiles into the United States from his native China.

Yi Qing Chen of Rosemead was convicted in October of attempting to ship the shoulder-fired QW2 missiles as well as launch and operational hardware to a man who turned out to be an undercover FBI agent. He was arrested in 2005 before the missiles could be delivered.

"The defendant's willingness to smuggle surface-to-air missiles into this country or anywhere is a frightening concept because there can be no confusion as to the purpose of such contraband," said Steven Martinez, assistant director in charge of the FBI's Los Angeles office.

In passing sentence, U.S. District Judge Dale S. Fischer said Chen "never saw a criminal scheme he didn't want a part of."

U.S. Attorney Andre Birotte Jr. said Chen, a naturalized U.S. citizen, was the first person indicted under a federal anti-terrorism statute adopted in 2004 as a result of the Sept. 11 attacks.

The law, which banned the importation of missile systems designed to destroy aircraft, calls for a mandatory minimum sentence of 25 years and a maximum of life in prison without parole.

Chen, 49, was among dozens of people arrested as the result of Operation Smoking Dragon, an undercover FBI investigation that targeted those suspected of trying to smuggle counterfeit currency, drugs and other contraband into the United States.

Authorities said the arrests have resulted in nearly three dozen convictions in Los Angeles.

Evidence presented at Chen's trial, including tape-recorded conversations, showed he and a fellow conspirator, who has since died, told the FBI agent they had been involved in trafficking drugs, counterfeit cigarettes and other items from China. The agent was told they could supply as many as 200 anti-aircraft missiles.

Chen was also convicted of conspiracy to distribute cocaine and methamphetamine and of trafficking in counterfeit and contraband cigarettes. He was ordered to pay $520,000 to tobacco company Philip Morris USA.

Fired Gucci Network Engineer Charged for Taking Revenge on Company

http://news.softpedia.com/news/Fired-Gucci-Network-Engineer-Charged-for-Taking-Revenge-on-Company-193321.shtml

April 5th, 2011, 14:52 GMT| By Lucian Constantin

A computer network engineer who worked for Gucci America has been indicted after hacking into his former employer's computer systems and damaging data.

According to prosecutors, while working at Gucci, Sam Chihlung Yin, 34, of Jersey City, created a VPN USB token in the name of a fictional employee. After being fired in May 2010, Yin contacted the company's IT department posing as that employee and asked for his token to be activated.

In the months that followed Yin used his knowledge to repeatedly caused damage to Gucci's operations by disabling servers, locking documents and deleting emails.

In one instance, on November 12, 2010, during the course of two hours, Yin deleted several virtual servers, shut down a storage area and wiped clean an entire disk from the company's email server.

These actions have resulted in severe disruptions to daily activities, not only for Gucci's staff at the company's Manhattan headquarters, but also store managers across the country who couldn't access their emails.

The damages sustained by Gucci as a result of loss productivity, attack mitigation and data restoration is estimated at $200,000.

Yin has been indicted on 50 counts of computer tampering, identity theft, falsifying business records, computer trespass, criminal possession of computer related material, unlawful duplication of computer related material and unauthorized use of a computer.

"Computer hacking is not a game. It is a serious threat to corporate security that can have a devastating effect on personal privacy, jobs, and the ability of a business to function at all. This Office's Cybercrime and Identity Theft Bureau is committed to preventing and prosecuting crimes such as the one charged in today's indictment," said Manhattan District Attorney Cyrus R. Vance, Jr.

Belgians charged with smuggling aircraft parts

http://www.fresnobee.com/2011/05/17/v-print/2391946/belgians-charged-with-smuggling.html

Posted at 04:41 PM on Tuesday, May. 17, 2011

The Associated Press
SAN DIEGO Two Belgian men smuggled millions of dollars' worth of helicopter and aircraft parts from the United States to Iran, according to a federal grand jury indictment.

The indictment alleges that Willy De Greef, 70, and Frederic Roland Nicolas Depelchin, 39, sent the parts to unidentified customers through their companies, Meca Airways Ltd. and Meca Overseas Airways Ltd, which were also named as defendants.

The U.S. attorney's office in San Diego said Tuesday that De Greef was arrested Friday in London by the Metropolitan Police, and the United States will seek extradition. Depelchin is at-large.

The defendants were charged with attempted export to an embargoed country, conspiracy, wire fraud, smuggling and money laundering. De Greef is also charged with making false statements.

It was not immediately clear if De Greef or Depelchin had attorneys.
The grand jury indictment was handed up in March and unsealed Friday. It alleged the Belgian brokers concealed from U.S. suppliers that the parts were

going to Iran - a violation of federal law unless authorized by the Treasury Department.

The parts cited in the indictment included helicopter switches, fuel cells and turbine bypass valves.

TECHNIQUES, METHODS, TARGETS

How a networking immigrant became a spy

http://news.yahoo.com/s/ap/20110508/ap_on_re_us/us_stealing_for_china_the_networker/print

By PAULINE ARRILLAGA, AP National Writer

Sun May 8, 1:13 pm ET

Locked in a federal penitentiary in the Arizona desert, Tai Kuo spends his days helping with the cooking, teaching language classes and tennis, making new friends.

The convicted spy, it seems, has become a mentor.

This surprises no one. Not the prosecutors who charged him. Not his old friends or colleagues, some of whom stand behind him still.

Because Tai Kuo is nothing if not likable. It's the very quality that allowed him to get close to people in high places. Politicians. Army brass.

His attorney, Plato Cacheris, says, "We have represented over the years a lot of scoundrels." But Kuo "is not in that category. ... You always wanted to help him, if you will."

He wasn't a professional agent by any means. He was a tennis coach. A restaurateur. A businessman who lived with his wife and daughter in a Louisiana town known for swamp tours and charter fishing. Born in Taiwan, son-in-law of a senior military officer there, he was an unlikely spy for China if ever there was one.

And yet his journey from entrepreneur to secret operative — one of dozens convicted in the last three years of efforts to pass secrets or restricted

technology to the Chinese — is, in many ways, emblematic of the way China conducts espionage in the 21st century, experts say.

It is rooted in opportunity, nurtured by perseverance, sustained by greed. It relies on "guanxi" — a you-scratch-my-back, I'll-scratch-yours notion of developing close relationships.

The Chinese took advantage of all of these things to cultivate Kuo, and then the man with the winning personality went to work on their behalf. In the end, Kuo would convince two U.S. government employees to give him secret information, which he then conveyed to an official with the communist nation.

His networking skill would make Kuo wealthy, a shining immigrant success story, but it would also make him a convicted felon — a man denounced by a bitter ex-friend as "worse than a thief ... a traitor."

Even in his youth, Kuo (pronounced gwoh) knew how to forge connections with people who mattered. In his early 20s, still living in his native Taiwan, he worked as a tennis instructor for the U.S. Embassy in Taipei. He soon obtained a student visa and landed in Cajun country in 1973, attending Nicholls State University in Thibodaux, La., on a tennis scholarship.

Southern Louisiana became his home. Kuo graduated with a degree in business administration and accounting, married a woman from Taiwan, became a U.S. citizen and settled with his wife in Houma, La., where he set about becoming a successful entrepreneur. He ran a tennis club, taught Chinese cooking lessons and oversaw the restaurant at the Houma country club before launching his own high-end Chinese eatery — "Mr. Tai's" — in New Orleans.

The late 1980s saw his circle of connections widen. With China growing more open to foreign investments, Kuo started a business working to market American expertise and products there. He teamed with a Louisiana legislator to sell cotton, promoted oil service companies for exploration work in the South China Sea, provided engineers for the development of Chinese plants.

"He was the matchmaker," says David Crais, former chairman of the Louisiana Imports and Exports Trust Authority, to which Kuo was appointed in 1992. "He was a wheeler-dealer kind of guy who had major contacts. He was tapped into everybody."

Crais recalls Kuo promising potential clients, "I'll get you in China," and he knew how to do it.

"He used to say there's a billion people, but there's a very small group that runs the whole show. If you tapped into the power networks, that's where you got business done."

Apparently, the center of Kuo's power network was a man named Lin Hong. A friend introduced the two, telling Kuo, "He's a good person to know," someone who could help potential North American investors in China.

Hong, according to court papers, worked for the Guangdong Friendship Association, one of many groups in China whose stated aims are to promote good relations with foreign countries and organizations. The association is backed by the Chinese government and hosts visits for private individuals and businesspeople. But foreign researchers have also tied the friendship groups to present-day efforts to collect intelligence.

Guangdong association did not immediately respond to faxed and telephoned queries about whether it has ever employed a Lin Hong.
As Kuo's travel to China increased, he'd stop in the province of Guangdong and meet with Hong, who loved to talk.

"Lin always was very, very (interested) about the attitude of Congress toward China, the attitude of U.S. government to Chinese, the relationship between the U.S. and Taiwan ...," Kuo would later testify.

Kuo considered Hong a friend, at least at first. However, U.S. investigators use a different description. Hong, they say, was Kuo's "handler," who for years tasked Kuo with gathering information from contacts he'd made in the U.S. government. It started with a request for "opinion papers." Hong knew that Kuo was tight with various politicians and government officials. He wondered if Kuo could find someone to write papers to help him better understand U.S. attitudes toward China.

Kuo turned to a retired Air Force lieutenant colonel named Jim Fondren, who was from Houma and had gotten to know Kuo through the country club. Fondren's area of expertise was Asia, after having worked doing strategic planning for the United States Pacific Command (PACOM), the senior U.S. military authority in the Asia-Pacific region.

Sometime around 1997, Kuo approached Fondren about writing papers for Hong, whom he described, at Hong's suggestion, as working at an academic entity in Hong Kong.

Fondren, who was trying to launch a consulting business, received anywhere from a few hundred dollars to $1,500 for his papers. He was treated to a trip to

China, where he, Kuo, Hong and Hong's boss played golf in the coastal town of Zhuhai and took a boat trip through picturesque Guilin.

"May our friendship last long and welcome you back again," Hong inscribed in a keepsake book that he gave to Fondren.

Kuo, meanwhile, was currying favor with Hong, who he hoped would help him land a project in China. Kuo would later acknowledge his own motivation: "Just pure and simple greed."

Then something happened that gave Hong more leverage over Kuo. Around 2002, some Chinese engineers who worked with Kuo on a project in Taiwan were arrested upon their return to China and accused of espionage. Kuo turned to Hong to help get them out of prison.

After that, Kuo would say later, Hong got more pushy.

"`You go to Washington more often,'" he testified Hong demanded, and the things he wanted were sometimes "very sensitive."

And as Hong put more pressure on Kuo, Kuo put more pressure on Fondren — who, as it happened, had returned to work with the U.S. government in 2001. He was based inside the Pentagon as the deputy director of the Washington liaison office of PACOM, a position that granted him "Top Secret" security clearance.

Fondren continued to produce opinion papers about such topics as visits of senior Chinese military officials to the United States, talks between the Department of Defense and China's People's Liberation Army, a joint exercise conducted between the U.S. and Chinese navies. One paper incorporated information from a Department of Defense report classified as "confidential." Fondren also provided various publications, including a draft copy of an annual Defense report on the People's Liberation Army.

To help convince Fondren to keep giving him information, Kuo — at Hong's suggestion — told him his papers were now going to government officials in Taiwan rather than to Hong.

Kuo would use the same approach in wooing a second tipster.

The FBI videotape shows the inside of a rental car, with Kuo in the passenger seat. He pulls out a wad of cash, the outer bill being a $100 note. Then Kuo stuffs the money into the shirt pocket of the driver, Gregg Bergersen, and the two proceed to talk business.

"Now, the other information ... I'm very, very, very, very reticent to let you have it because it's all classified ...," Bergersen tells him. "But I will let you see it and you can take all the notes you want. ... But if it ever fell into the wrong hands, and I know it's not going to ... then I would be fired for sure. I'd go to jail, because I violated all the rules."

The two then stop for lunch, and Bergersen hands Kuo a thick document with cut marks at the top and bottom of each page; he explains that he's removed the classification markings. For an hour at the restaurant, Kuo takes notes from the document, which details the quantity, dollar value and names of weapons systems planned for sale by the United States to Taiwan for five years.

It was July 14, 2007, and Kuo was on one of his many information-gathering trips to Washington, D.C. It had been a decade since he started passing information to China.

Bergersen worked as a weapon systems policy analyst at the Defense Security Cooperation Agency, an arm of the Department of Defense that facilitates military sales overseas. His specialty was C4ISR, a sophisticated military command, control and communications network.

As one of his many business enterprises, Kuo was pursuing contracts with Taiwan related to its version of C4ISR, known as Po Sheng or "Broad Victory." By 2004, he and Bergersen had formed a business relationship. Bergersen wanted to promote C4ISR in Taiwan and believed Kuo could help. The two would go to dinner, with Kuo picking up the tab. They discussed going into business upon Bergersen's retirement, and Kuo promised a job with a six-figure salary. They traveled to Las Vegas, and Kuo gave Bergersen gambling money and show tickets.

In return, Bergersen supplied Kuo with classified information related to Po Sheng and other U.S. defense technology and communications systems, which Kuo then gave to Hong.

Kuo began using encryption software to send e-mails and also enlisted a "cutout" — a young woman who had worked with him in the furniture import business and with whom he began having an affair — to sometimes serve as a go-between with him and Hong.

To avoid detection, Hong suggested that Kuo buy prepaid phone cards and use public telephones. He wanted him to change his e-mail addresses often, mail documents to him from the airport or another public location. For the most part, Kuo ignored his advice.

He'd later testify that he was "just ignorant, I guess. Arrogant. I didn't think I can get caught."

But FBI agents had stumbled upon Lin Hong's name in a separate investigation of a California engineer who illegally exported military technology to China. Investigative work in that case led to Kuo, and agents began planting recording devices in his rental cars and watching his Internet activity. They also bugged Fondren's home, and watched Bergersen.

On Feb. 11, 2008 — almost two decades after first meeting Lin Hong — Kuo was arrested and charged with espionage.

Quickly pleading guilty, he began cooperating with the government.

He testified against his old friend Fondren, helping convict him of communicating classified information to an agent of a foreign government and making false statements to the FBI.

On the stand, Fondren himself said: "I had no idea that the guy that I thought was one of my best friends, one of the great American success stories, was worse than a thief. He's a traitor to this country. ... I'm the first to salute the government for getting him."

Sentenced in 2010 to three years, Fondren remains in a federal penitentiary in Pennsylvania. He did not respond to written requests to be interviewed.

Bergersen, who was arrested the same day as Kuo, pleaded guilty to conspiracy to communicate national defense information and was sentenced to almost five years in prison, although he is scheduled to be released to home confinement in Texas by the end of June. He maintains that he did not act for financial gain but rather to help promote the defense system he'd spent years working on.

"I deluded myself into believing it was acceptable to act illegally for good results," Bergersen said in a written testimonial forwarded to The Associated Press by his cousin. In it, he says his behavior also was fueled by an addiction to alcohol. "I know now that I was not deceived by Kuo's lies and deceptions but by my own sins."

In the end, the information Fondren and Bergersen passed to Kuo caused little or no harm to national security, their sentencing judges determined. But that does little to minimize Kuo's actions in the eyes of his family or former friends. His wife divorced him, and his daughter won't speak to him, according to friends.

"I don't know what happened to Tai, other than he was the victim of my invincibility theory," says Danny Lirette, a Houma attorney who remains close to Kuo and speaks with him regularly. (Kuo declined to be interviewed by the AP.)

"I see all these people who become very powerful and accumulate wealth and are surrounded by people who tell them how great they are. They think they can do whatever they want. That's when they fall to the bottom."

Initially, Kuo was sentenced to nearly 16 years in prison, but that was reduced last summer to five years — thanks to his cooperation with authorities. Lirette says he could be released to a halfway house by the end of this year, and that he'll find a way to start again.

"He's going to be fine," says Lirette. "He'll have some struggles. But Tai ... he doesn't give up."

EDITOR'S NOTE — This story is based on interviews with Justice Department officials, Kuo's attorneys and friends, and a review of court documents in the Kuo, Bergersen and Fondren cases, including testimony at Fondren's trial.

Shriver Case Highlights Traditional Chinese Espionage

http://webcache.googleusercontent.com/search?q=cache:s2gpVz_ZRb4J:www.jamestown.org/programs/chinabrief/single/%3Ftx_ttnews%255Btt_news%255D%3D37143%26tx_ttnews%255BbackPid%255D%3D414%26no_cache%3D1+picture+of+chi+mak+greg+chung&cd=7&hl=en&ct=clnk&gl=us&source=www.google.com

Publication: China Brief Volume: 10 Issue: 22
November 5, 2010 06:44 PM

Category: China Brief, Home Page, Foreign Policy, Military/Security, China and the Asia-Pacific

By: Peter Mattis

Underneath the fanfare that greeted the FBI's arrest of ten Russian intelligence officers in June, federal authorities quietly proceeded against a young Michigan man, Glenn Duffie Shriver, applying to the CIA at the direction of Chinese intelligence. The story missed major media outlets and was almost exclusively covered by local press. On October 22, Shriver pled guilty to the charges and agreed to cooperate with the FBI (Detroit Free Press, October 22). Consistent with Chinese policy on not acknowledging foreign intelligence operations, the

Chinese embassy spokesman in Washington officially denied any connection to Shriver, emphatically stating that "China would never involve itself in activities damaging to another country's interest." In a press interview related to the case, one Chinese scholar affiliated with the Ministry of State Security went further, implying Shriver was implicating China to reduce his punishment (Global Times [Beijing], October 25).

As the most recent in a string of Chinese espionage arrests, the Shriver case could be another important data point for analyzing trends in Chinese intelligence operations against the United States [1]. The facts available are sparse and undoubtedly more information will come out, but the case already challenges some widespread views about Chinese intelligence that could shed light on conventionally held beliefs about its operations. The Shriver case also presents a modern example of Chinese seeding operations that have been an integral component of Chinese Communist Party (CCP) intelligence since the early days of the CCP [2]. The historical continuity of the Shriver case with past operations underscores the need to analyze this incident carefully.

The Facts of the Shriver Case

On October 22, Shriver pled guilty to conspiring to provide national defense information to Chinese intelligence and will be sentenced in January. He will most likely face four years in prison, assuming he cooperates with the FBI, according to the Department of Justice.

Shriver studied in China during the 2002-2003 school year as an undergraduate, but left when SARS hit. When he moved back to Shanghai in 2004, Shriver responded to an advertisement soliciting papers on Sino-American relations. Chinese intelligence—it still unknown whether this was a civilian or military organization—paid Shriver $120 dollars and proceeded to recruit him over the course of several meetings (Department of Justice, October 22).

Chinese intelligence first tried to direct Shriver into the State Department, but he failed the Foreign Service Officer exam twice. Still, Chinese intelligence paid him $30,000 for his efforts. In 2007, Shriver discreetly traveled to China and received another $40,000 as Chinese intelligence switched targets, directing him toward the CIA. Over the course of the application process, Chinese intelligence also met him in person roughly twenty times. In spring 2010, Shriver reported to Washington, D.C. for final processing to join the National Clandestine Service.

Apparently, at this time federal investigators confronted Shriver about inconsistencies in his statements—such as contact with foreign government organizations and his 2007 trip to China, of which even his mother was

unaware—and probably elicited a confession (Grand Rapids Press, June 25; Department of Justice, October 22).

Signaling a Possible Change in Chinese Intelligence Operations

The Shriver case has several interesting features that challenge the conventional view in the United States that China practices intelligence in a fundamentally different way than Western or Russian intelligence services. This makes the Shriver case either an outlier or an exception that disproves the rule.

The conventional view of Chinese intelligence operations is sometimes referred to as the "thousand grains of sand" or "mosaic" approach to collection, characterized by broad-based, diffuse collection of predominantly unclassified information [3]. According to this view, the Chinese vacuum up high volumes of small pieces of intelligence to later assemble into a more complete picture back in China. Instead of paying assets, Chinese intelligence prefers to target ethnic Chinese who can be pressured or appealed to on patriotic grounds; foreigners can be leveraged through positive moral inducements, sometimes so subtly they are unaware of Chinese efforts to gather intelligence [4].

The details of Shriver's case recounted above, however, do not suggest he is a mere "grain of sand" in a Chinese vacuum cleaner. Firstly, Shriver is obviously not ethnically Chinese and therefore could be appealed to based on patriotism or pressure on his family. Secondly, Chinese intelligence relied on his greed rather than positive moral inducements, meaning the intelligence service was willing to pay for the chance to access classified information and promised to continue payment if he gained access to national security information (Department of Justice, October 22). One wonders if Shriver was promised a bonus if he successfully became employed with the CIA or another national security organization, which would have provided an even clearer indication that the Chinese are, at least now, willing to exchange dollars for documents. Thirdly, Chinese intelligence was trying to seed him into the CIA, which is not exactly the low-hanging fruit of sensitive US Government information. CIA and NSA are well known around the U.S. national security establishment for having the most rigorous screening processes for employees.

One case does not disprove a hypothesis; however, it warrants looking back at the history of modern Chinese intelligence operations to see whether the Shriver case represents continuity. The extent to which this case reflects past Chinese operations adds to the weight we should give this as a counter-example to conventional views of Chinese intelligence being exceptional to Western and Russian practices.

"Long Tan San Jie": The Birth of Modern Chinese Seeding Operations

Analysts could cite China's first spy, Yi Yin, who infiltrated Xia Dynasty to collect intelligence for the rising Shang Kingdom, or Sun-Tzu's manipulation of "living" or "expendable" spies for historical Chinese examples similar to Chinese intelligence's efforts to seed Shriver into the CIA [5]. More recently and relevantly, seeding operations go back to the earliest days of the Chinese Communist Party (CCP) as it struggled to survive its competition with the Kuomintang (KMT) in the 1920s. In the late 1920s, then CCP intelligence chief and future premier, Zhou Enlai, and operations chief Chen Geng directed Hu Di, Li Kenong, and Qian Zhuangfei to infiltrate the KMT in Tianjin, Shanghai, and Nanjing, respectively [6]. These three spies provided crucial warning to the CCP during the peak of the KMT's White Terror in 1931, which arguably saved what was left of the CCP.

All three successfully gained employment with and access to sensitive KMT information, most notably Li and Qian as members of the KMT's cryptological and radio intercept units. Hu took a position under cover as a journalist with the Great Wall Daily, which served as a front for the central office of the KMT intelligence section in Tianjin. For the three years between their successful infiltration of the KMT and their critical moment, Hu, Li, and Qian provided warning intelligence on the KMT's increasingly sophisticated and targeted efforts to eliminate underground CCP cells across China. They also provided insight to CCP leaders on KMT methods and capabilities, enabling better CCP counterintelligence practices to deny the KMT information. The most notable of the three, Qian Zhuangfei, rapidly demonstrated his competency for the KMT and became the private secretary to Xu Enzeng, then head of the KMT intelligence apparatus [7].

The critical success came on April 25, 1931, when Qian's position as private secretary to Xu arguably saved the CCP. On that day, KMT security officials in Wuhan arrested one of the CCP Special Department's four operational directors, Gu Shunzhang, and persuaded him to defect. Ignoring Gu's warning about a high ranking penetration, the KMT security officer telegraphed Xu the good news about Gu's willingness to cooperate. Qian was the first to receive the telegraph and delayed passing the telegram to Xu, instead sending word Li in Shanghai. This warning prior to Gu's arrival to and debriefings in Nanjing gave the CCP roughly an 18-hour head start to salvage their Shanghai apparatus before KMT authorities began cracking down. Future leaders, such as Zhou Enlai, successfully evaded capture, although the damage further weakened a CCP stricken by the KMT's "White Terror" [8].

"We sent these men into the dragon's lair and the tiger's den (long tan hu xue)," Zhou Enlai stated, "without the 'three heroes of the dragon's lair' (long tan san jie), the history of the CCP would have to be rewritten" (Beijing Keji Bao, December 3, 2004). This historical vignette is one of the founding stories of

modern Chinese intelligence, kept alive through popular historical articles, documentaries and books. It may also have some relevance to Chinese operational methods—at least in terms of operational timelines and patience—since Li Kenong became a leading figure in Chinese intelligence from 1942 until his death in 1962.

Modern Seeding? The Case of Chi Mak

In the more recent past, Chinese intelligence also directed Chi Mak from his emigration from China through his long journey to U.S. citizenship and access to sensitive U.S. military engineering projects, according to the FBI's affidavit. Mak left China for Hong Kong in the 1960s and onto the United States in 1978. Arrested in 2005 and convicted in 2007, Chi Maki's intelligence activities span more than three decades—during most of which he did not have direct access to sensitive information (Washington Post, April 3, 2008).

Mak's first projects on behalf of Chinese intelligence were relatively innocuous. While in Hong Kong, Mak reportedly kept logs of U.S. warships making port calls in the British territory. In 1986 and after immigrating to the United States, Chinese intelligence asked Mak to serve as a courier for Dongfan "Greg" Chung, who was convicted in 2009 for economic espionage and acting as an unregistered agent of a foreign power. Not until Mak became a citizen in 1985 was he in a position to get a security clearance—which he got in 1996—and gain access to U.S. military secrets (Affidavit in USA v. Chi Mak, October 2005; New York Sun, March 23, 2007).

After gaining his secret clearance, Mak worked on classified and unclassified projects for the U.S. Navy at Power Paragon, a subsidiary of L-3 Communications / SPD Communications / Power Systems Group. Chinese intelligence provided at least two lists of US technologies for Mak to acquire information on, including data on the Quiet Electronic Drive, DD(X)-related, and other advanced naval technologies (Affidavit; Washington Post, November 16, 2005).

Mak and Shriver demonstrate the willingness of Chinese intelligence to invest time into agents who do not have immediate access to important or sensitive information. This is not the patience of putting tiny bits of information together, but the patience of waiting for opportunities. Yet, these two recent examples differ from the "long tan san jie" in one vital respect. Mak and Shriver were recruited agents of Chinese intelligence, whereas Hu, Li, and Qian were officers of the CCP intelligence apparatus. This begs the question of whether Chinese intelligence today still dispatches its officers to infiltrate sensitive intelligence targets and the role of the party in intelligence gathering.

Trying to repeat the exploits of the "long tan san jie" against foreign governments today would be substantially more difficult—or at least more time-consuming—than infiltrating the KMT. First, the target country would have to be one that allows immigration and willing to admit immigrants into its national policymaking structure, such as Canada and the United States. Second, the Chinese intelligence officer would have to qualify for immigration and be properly processed (possibly for years!). Third, that officer would have to pass the targeted country's vetting system without alerting security officials in the process or have other issues disqualifying the officer. Given the relative secrecy of such vetting methods, this process could require a lot of expensive and frustrating trial-and-error if Chinese intelligence was starting without a baseline. Indeed, there is not a single public example of Chinese intelligence trying to seed its officers against foreign targets. Yet, no doubt counterintelligence officials both in the United States and abroad have their own ideas and sources.

Conclusions

The Shriver case's continuity with the past, albeit with variations, suggests we should be open to revising the view that Chinese intelligence operates along the "thousand grains of sand"- or "mosaic"-model of operations. The Chinese intelligence organization directing him toward the CIA had clear intent to exploit his future access to sensitive US Government information, as demonstrated by the $70,000 down payment. The information Shriver might have had access to at the CIA could have provided actionable lead information for Chinese counterintelligence investigations, a sense of the US technical collection posture against China and Intelligence Community intelligence products. These are not the proverbial sand grains indiscriminately gathered for central processing.

From what little has been made public about this case, we are left to wonder about several key details. First, did Shriver's case officers meet him overseas? Although this sounds like an obvious question with an obvious answer, most of the publicized Chinese espionage cases from Bernard Boursicot (also known as the M. Butterfly case) to the more recent James Fondren (a U.S. Defense Department official) involved Chinese case officers who were based in mainland China [9]. Because Shriver only went back to China once since 2004, this question is not academic. If Shriver was not being met in person inside China, then how was Chinese intelligence communicating with him and how did they plan to communicate with him if he slipped past CIA security? Were the Chinese case officers traveling overseas to meet Shriver (a noteworthy development itself!) since they apparently met several times possibly after Shriver's last trip to China several years ago?

Further analysis will be required as more information comes to light. However, the implications of the Shriver case have more practical applications than an

understanding of Chinese intelligence operations. American and other foreign students traveling to and studying in China should be cognizant that the Chinese intelligence services are watching. This particularly applies to those students with scholarship obligations to the U.S. government. Former Chinese intelligence and security officials speaking publicly in recent years have highlighted how the services use a network of intelligence officers and Chinese "friends" in universities, municipal government and the entertainment industry to identify potential sources or lure them into compromising positions (Sydney Morning Herald, June 9, 2005; Taipei Times, December 17, 2005). While most visitors to China have an appreciation that they might be wandering through a fishbowl, the Shriver case provides a concrete example of how an individual's weaknesses can be identified and preyed upon.

Notes

1. Prior to 2005, the United States had arrested and prosecuted only two Chinese spies, Larry Wu-Tai Chin and Wu Bin, who were confirmed to be working on behalf of Chinese intelligence. Since that time, the FBI has linked Chi Mak and his family, Dongfan "Greg" Chung, Kuo Tai-Shen, Gregg Bergersen, Kang Yuxin, and James Fondren to Chinese intelligence with sufficient proof to stand up in a courtroom. Other unmentioned cases were never proved conclusively or sufficiently by U.S. legal standards.

2. Patrick Tyler, "Cloak and Dragon; There is No Chinese James Bond. So Far," New York Times, March 23, 1997. Former chief of FBI Counterintelligence Harry Godfrey III said "We have seen cases where they have encouraged people to apply to the CIA, the FBI, and Naval Investigative Service, and other Defense agencies."

3. "Special Report: Espionage with Chinese Characteristics," StratFor Global Intelligence Report, March 24, 2010; Paul Moore, "How China Plays the Ethnic Card: Beijing's Strategy of Targeting Chinese Americans is Hard to Counter With US Security Defense," Los Angeles Times, June 24, 1999; Jeff Stein, "Espionage without Evidence: Is It Racism or Realism to Look at Chinese-Americans When Trying to Figure Out Who's Spying for China?" Salon.com, August 26, 1999; Peter Grier, "Spy Case Patterns the Chinese Style of Espionage," Christian Science Monitor, November 30, 2005.

4. Moore, "For Both, Spies are Inscrutable" Wilmington Morning Star, 30 August 2001, p. 11A; "Special Report: Espionage with Chinese Characteristics," StratFor: 12; 2009 Annual Report to Congress, US-China Economic and Security Review Commission, 149; Hamish McDonald, "Spying the Chinese Way: Millions of Snippets from All Over the World," Sydney Morning Herald, June 6, 2005.

5. Li Mingyang, ed., Sunzi Bingfa [Sun-Tzu's Art of War], Hefei, Anhui: Huangshan Shushe [Yellow Mountain Books] (2001): 193-194; Ralph Sawyer, The Tao of Spycraft: Intelligence Theory and Practice in Traditional China, Boulder, CO: Westview Press (2004): 7-12.

6. Frederick Wakeman, Policing Shanghai 1927-1937, Berkeley, CA: University of California Press (1996): 138-142; Xu Linxiang, Li Kenong Zhuan, Hefei: Anhui People's Press (1997): see Chapter 1 Sections "Chengwei Hongse Tegong" and "Long Tan San Jie de Shouci Xiangju".

7. Xu Linxiang, Li Kenong Zhuan, see Chapter 1 Sections "Long Tan San Jie de Shouci Xiangju" and "Qiequ Qingbao"; "Zhonggong Long Tan San Jie: Qian Zhuangfei, Li Kenong, Hu Di," Beijing Keji Bao, December 3, 2004.

8. Wakeman, Policing Shanghai 1927-1937, 151-160; Xu, Li Kenong Zhuan, see Chapter 2 Sections "Gu Shunzhang Panbian" and "Dui Gu Shunzhang Caiqu Cuoshi".

9. Joyce Wadler, "The True Story of M. Butterfly – The Spy Who Fell in Love with a Shadow," The New York Times Magazine, August 15, 1999; Neil Lewis, "Chinese Espionage Cases Raising Concerns in Washington," New York Times, July 10, 2008; Superseding Criminal Indictment in United States v. James Wilbur Fondren, US District Court for the Eastern District of Virginia – Alexandria Division, August 2009.

Condé Nast got hooked by $8 million spear-phishing scam

http://arstechnica.com/tech-policy/news/2011/04/conde-nast-got-hooked-by-8-million-spear-phishing-scam.ars

By Kim Zetter, wired.com | Published about a month ago
Bebeto Matthews/AP

A spear-phisher managed to reel in a prize catch last year with a single hook when media giant Condé Nast took the bait and wired $8 million to his bank account after he posed as a legitimate business, according to a news account. The alleged swindler failed to withdraw any funds before federal authorities intervened and froze the money, but the case highlights how little effort a scammer needs to invest in order to get a big payday.

A Condé Nast representative said the company could not comment on a pending investigation. Condé Nast publishes Wired magazine and Wired.com, as well as Vogue, The New Yorker, GQ, Glamour, and Ars Technica.

Information about the scam appeared in a forfeiture lawsuit filed March 30 in Manhattan by the US Attorney's office for the Southern District of New York in an attempt to retrieve the money for Condé Nast. It was first reported by Forbes.

The filing seeks the funds for forfeiture on grounds that they are allegedly proceeds from wire fraud and money laundering crimes.

According to the court document, last November Condé Nast's accounts payable department received an e-mail (PDF) that purported to come from Quad/Graphics, the company that prints Condé Nast magazines.

The e-mail instructed Condé Nast to send payments for its Quad/Graphics account to a bank account number provided in the e-mail, and included an electronic payments authorization form. The e-mail indicated the account was for Quad Graph, a name similar to the real printer's name.

Someone at Condé Nast apparently signed the form and sent it back to a fax number listed in the e-mail, then began making electronic transfer payments to the bank account specified by the scammer.

Between Nov. 17 and Dec. 30, the company wired $8 million to the Quad Graph account before a query around Dec. 30 from the real printer, Quad/Graphics, asking about outstanding bills, prompted Condé Nast to investigate the matter. The company was apparently able to reverse at least one transfer of about $36,000 back to its JPMorgan Chase account, though the court document doesn't indicate when that occurred.

According to the court filing, a man named Andy Surface allegedly opened the scam bank account last September at a branch of BBVA Compass Bank in Alvin, Texas. Surface had allegedly incorporated his business name with the county clerk's office before opening the bank account, identifying his home address in Alvin as the location of the business.

During December, about $84,000 of the $8 million was transferred from the Quad Graph account into another account bearing Surface's own name, but no money was withdrawn from either account before federal authorities got wind of the operation. They obtained a federal seizure warrant on January 10 to freeze the funds until they could file the forfeiture lawsuit to retrieve them.

Surface has yet to be charged with any crime related to the scam, but Forbes dug up a previous charge against someone with the same name and address who pleaded no contest in December to "terroristic threat of family/household." The US Attorney's office declined to comment.

Exclusive: Inside Area 51, the Secret Birthplace of the U2 Spy Plane

http://www.foxnews.com/scitech/2011/05/17/book-excerpt-area-51-uncensored-history-americas-secret-military-base/?intcmp=sem_outloud&intcmp=obnetwork

Published May 17, 2011

FoxNews.com

The crash of a disc-shaped aircraft in Roswell New Mexico, in July 1947 kicked off UFO speculation worldwide. In fact, the disc was a Russia spy plane, reveals Annie Jacobson in the new book "Area 51."

In her new book "AREA 51: An Uncensored History of America's Top Secret Military Base," which goes on sale May 17, Annie Jacobsen offers for the first time an inside look at the history of America's top secret military base. It is the first book based on interviews with the scientist, pilots, and engineers -- 74 in total -- who for the first time reveal what really went on in the Nevada desert, from testing nuclear reactions to building super-secret supersonic jets to pursuing the war on terror.

Jacobsen, a contributing editor and investigative reporter at the Los Angeles Times Magazine, interviewed the former Area 51 employees in 2008 and 2009, shortly after the CIA declassified much of the work they had done, including countless pages of redacted memos and declassified reports. Area 51 is still officially a military secret, unmentioned by name, Jacobsen notes.

In this exclusive excerpt, Jacobsen reveals some of the wild research that went on in the 1970s at Area 51 -- where the military built the U-2 spy plane, rather than harboring crashed UFOs.

Chapter 20: From Camera Bays to Weapons Bays

By 1974, the Central Intelligence Agency had ceded control of Area 51. Some insiders say the transition occurred in 1979, but since Area 51 does not officially exist, the Air Force won't officially say when this handover occurred.

An inside look at the history of America's top secret military base, the nonfiction book "Area 51" includes 74 first-hand eyewitnesses linked to the secret base. Certainly this had to have happened by the time the stealth bomber program was up and running; the F-117 program was the holy grail of Pentagon black projects — and, during that time period, the Air Force dominated Area 51.

Having no business in bombs, the CIA maintained a much smaller presence there than historically it had before. During the 1970s, the Agency's work concentrated largely on pilotless aircraft, or drones. Hank Meierdierck, the man who wrote the manual for the U-2 at Area 51, was in charge of one such CIA drone project, which began in late 1969.

Code-named Aquiline, the six-foot-long pilotless aircraft was disguised to look like an eagle or buzzard in flight. It carried a small television camera in its nose and photo equipment and air-sampling sensors under its wings. Some insiders say it had been designed to test for radiation in the air as well as to gather electronic intelligence, or ELINT. But Gene Poteat, the first CIA officer ever assigned to the National Reconnaissance Office, offers a different version of events.

"Spy satellites flying over the Caspian Sea delivered us images of an oddly shaped, giant, multi-engine watercraft moving around down there on the surface. No one had any idea what this thing was for, but you can be sure the Agency wanted to find out."

"That is what the original purpose of Aquiline was for," Poteat reveals. "To take close-up pictures of the vehicle so we could discern what it was and what the Soviets might be thinking of using it for. Since we had no idea what it was, we made up a name for it."

"We called it the Caspian Sea Monster," Poteat explains. Project Aquiline remains a classified project, but in September of 2008, BBC News magazine produced a story about a Cold War Soviet hydrofoil named Ekranopian, which is exactly what the CIA's Aquiline drone was designed to spy on.

At Area 51, Hank Meierdierck selected his former hunting partner Jim Freedman to assist him on the Aquiline drone program. "It flew low and was meant to follow along communication lines in foreign countries and intercept messages," Freedman says. "I believe the plan was to launch it from a submarine while it was waiting in port." The Aquiline team consisted of three pilots trained to remotely control the bird, with Freedman offering operational support.

"Hank got the thing to fly," Freedman recalls. Progress was slow and "it crash-landed a lot." The program ended when the defense contractor, McDonnell Douglas, gave a bid for the job that Meierdierck felt was ninety-nine million dollars over budget. McDonnell Douglas would not budge on its bid, so Hank recommended that the CIA cancel Project Aquiline, which he said they did.

After the program was over, Hank Meierdierck managed to take a mock-up of the Aquiline drone home with him from the area. "He had it sitting on his bar at his house down in Las Vegas," Freedman recalls.

Project Aquiline was not the CIA's first attempt to gather intelligence using cover from the animal kingdom. Project Ornithopter involved a birdlike drone designed to blend in with nature by flapping its wings. And a third, even smaller drone was designed to look like a crow and land on windowsills in order to photograph what was going on inside CIA-targeted rooms.

The tiniest drone program, orchestrated in the early 1970s, was Project Insectothopter, an insect-size aerial vehicle that looked like a dragonfly in flight. Insectothopter had an emerald green minifuselage and, like Ornithopter, flapped its wings, which were powered by a miniature engine that ran on a tiny amount of gas. Through its Office of Research and Development, or ORD, the CIA had also tried turning live birds and cats into spies.

In one such program, CIA-trained pigeons flew around Washington, DC, with bird-size cameras strapped to their necks. The project failed after the extra weight tired out the pigeons and they hobbled back to headquarters on foot instead of in flight. Another CIA endeavor, Acoustic Kitty, involved putting electronic listening devices in house cats.

But that project also backfired after too many cats strayed from their missions in search of food. One acoustic kitty got run over by a car. The Agency's pilotless-vehicle projects were forever growing in ambition and in size. One robotic drone from the early 1970s, a project financed with DARPA, was disguised to look like an elephant —ready to do battle in the jungles of Vietnam.

ABOUT THE AUTHOR: ANNIE JACOBSEN is a contributing editor at the Los Angeles Times Magazine and an investigative reporter whose work has also appeared in the National Review and the Dallas Morning News. Her two-part series "The Road to Area 51" in the Los Angeles Times Magazine broke online reader records and remained the "most popular/most emailed" story for ten consecutive days.

Helping an Attorney Prove an Employee Theft/Theft of Trade Secrets Case with Computer Forensic Evidence: Part 1

http://www.dfinews.com/print/4840

Created 2010-05-28 10:10

By Bruce A. Olson

You've just received a call from an attorney who represents a company that learned one of its key employees is quitting to join a competitor. This employee had access to a proprietary database of sales and marketing information, key plans for future expansion, and trade secret information about the products the company manufactures and sells. The employee signed a non-compete agreement and a separate confidentiality agreement, but you have reason to suspect the former employee has no intention of abiding by these agreements. The employer wants immediate action and the attorney asks you what should be done.

Traditionally, the attorney would send a cease and desist letter to the former employee and the new employer based on the existing agreements, and then rush to the courthouse to file a motion for a temporary restraining order. Often they would do this without any hard evidence to back up the claim of the likelihood of irreparable harm. They would gather whatever documentary evidence they could find concerning information that was previously in the former employee's possession, and try to argue from the paper record and the fact the employee had access to computerized information on the client's computer network that the nature of the information the employee had access to could be used to aid the efforts of the new employer. If that happened they would contend the original employer would necessarily suffer grave commercial harm.

These days, however, a great deal more is required of an attorney before the motion for injunctive relief can be filed. You can help them meet their professional obligations by providing advice on the preliminary steps that need to be addressed to preserve electronically stored information. The attorney must first establish a litigation hold of all potentially relevant electronically stored information. Once this is done you will be in a position to examine the available electronic evidence in a forensically defensible manner to determine if there is actual proof that underlies the claim that the former employee took confidential information that can be used by the new employer to its financial advantage. Only then will the attorney be able to meet the evidentiary burden required when seeking a temporary restraining order against the use of such information. The attorney needs to have the technical expertise to manage these issues or he

needs to find someone who does who can quickly help him build the case. Thus, you may be able to help much sooner in the process than you might think.

Attorneys today know (or should know) that the duty to preserve electronic information arises when there is a reasonable expectation of litigation. When a key employee quits to go work for a competing employer there is little doubt there is a reasonable expectation of litigation. This means the employer contemplating litigation must immediately take steps to preserve the ESI. If the employee has a laptop or PC, the computer should be sequestered. If the employee gives notice in person during the work day, the employee should be accompanied back to his or her workstation and not be given access to the computer. If the computer is not turned on it should be left off, and the client should be warned not to allow anyone to boot it up until you've been to the site. If it is turned on, and you are not able to come to the site immediately, you should tell the client to pull the plug. You must explain to the attorney and the client that simply booting up the computer can alter potentially relevant ESI. Do not let the employee have any access to the computer. Check the employee's work area and look for thumb drives, data CDs, external drives, or other storage devices. Remember that these days even smart phones can be used as storage devices for large amounts of electronic information. If the employer provided cell phones for employee use, they too should be immediately seized. This should include seizure of any charging device, and the employer should be instructed that the phone should be kept charged until it is turned over to you for analysis. Explain that if a phone is allowed to lose its charge, potentially relevant data will be lost.

Your next thought should be about methods to preserve the employee's computer hard drive. The optimum solution is to have the hard drive forensically imaged by an appropriate professional. This should not be done by internal company IT personnel since they may lack appropriate expertise and may cause loss of data. Regardless, their objectivity will always be suspect. Do not let IT put the computer back into use by other employees before the evidence is secured. (You would be amazed how often this happens!) If a replacement employee is quickly hired who needs a computer, it is often cheaper to just buy a new computer given the problems a failure to properly preserve the evidence can cause. Barring that, you could clone the hard drive, and then install the copy in the computer while preserving the original hard drive as evidence. Documenting chain of custody about what you've done is very important and is another reason why outside experts who are properly trained should be used to secure computer data that will ultimately be used in litigation.

Once you've preserved the employee's computer there is much more to consider. Typically the employee used the computer to access information on the corporate network. This means some type of file server is implicated as a source

of potentially relevant ESI. In addition, the employee undoubtedly used e-mail, so an e-mail server is also something that needs to be addressed. Steps must be taken to ensure that no active data that may be relevant on either type of server is altered or destroyed. In addition, you must consider whether backup media needs to be preserved.

You must also immediately identify all potential sources of relevant electronically stored information and all custodians of information that need to be notified of their preservation obligations. The attorney must meet with the client's IT staff and take steps to ensure the ESI is preserved. Often it makes sense for you to participate in such a meeting to provide appropriate technical advice. The attorney must also generate a written plan for a litigation hold, see to it that it is appropriately disseminated, monitor compliance, and reissue the hold instructions on a periodic basis over the course of the ensuing litigation. Failure to address these issues properly can potentially result in sanctions against the attorney and the client.

Once proper steps to institute a general litigation hold have been taken you can turn to the employee's computer to determine whether it contains evidence of theft of proprietary information or other employee conduct that will support the claims for injunctive relief. You need to explain to the attorney why they need to retain a computer forensic examiner who knows how to properly preserve and analyze the ESI on the computer. There are defined steps that have become standard in the industry that must be followed to ensure the potential ESI is not altered, so it can be properly authenticated, and ultimately so it will be admissible in court. Too few attorneys understand these requirements.

Explain to them that in general a computer forensic examiner will use specialized equipment and/or software to create two bit for bit copies of the original computer hard drive. One copy is kept in pristine form to serve as a means to prove the ESI was properly copied and not altered in the copying process. The other copy—the working copy—is used by the examiner to conduct the analysis. In the process of making the forensic images write blocking hardware is typically used that ensures no data is written back to the original hard drive during the copying process. If such equipment isn't used, or alternatively, if specialized software and certain adjustments aren't made prior to the start of the imaging process, the copying process itself will alter data.

In addition, the source hard drive and the destination hard drive will be hashed, and a comparison of the hash values will be made at the end of the process. If the values are identical then the copy is forensically sound and no data alteration has occurred in the process. Explain that the hashing process applies a special algorithm that assigns a unique numerical value to the computer files, like an electronic fingerprint, that allows the original and copy to be compared. If any

changes are made to the data in the copying process the hash values will not be identical and the process will not be valid in terms of authentication of evidence. Attorneys must understand that this is a sophisticated process. They cannot drag and drop copies of files from the employee's computer to an external hard drive and obtain evidence that will be admissible in court. Doing so will alter metadata associated with the computer files and make their ability to show what the employee did impossible to prove with reasonable certainty. You should explain that a professional examiner will document the work by creating written chain of custody documentation and photographing the various steps of the imaging process thereby satisfying evidentiary authentication requirements for use of ESI in court.

Read more about using forensic software to analyze the evidence in Part 2.

Helping an Attorney Prove an Employee Theft/Theft of Trade Secrets Case with Computer Forensic Evidence: Part 2

http://www.dfinews.com/print/4834

Created 2010-06-02 15:34
By Bruce A. Olson
Part one of this article talked about how you can help attorney's meet their professional obligations by providing advice on the preliminary steps that need to be addressed to preserve electronically stored information in employee theft cases.

Only after these steps are completed can the actual data on the computer be analyzed using specialized forensic software. It is useful for the attorney to understand the typical types of information that can be gleaned from a forensic examination in an employee theft situation. The hard drive can be examined for any existing active files that are of proprietary nature. An examination of the file structure and file names are made since this can often demonstrate culpable conduct on the part of the employee. For example, the employee may have copied a key marketing memo by viewing the document on the network and then doing a save as to his local computer. To disguise the fact this proprietary information was copied, the saved file was named "vacationplans.doc" and was placed in a series of nested files that make it appear the file is personal in nature, e.g., C:/Documents and Settings/JoeSmith/VacationPlans/WisconsinDells_2010. When, during the course of the examination the examiner locates the memo using key word search techniques, the fact that the file was saved with this file name and in this file location provides evidence of culpable activity on the employee's part.

If the employee was a little more sophisticated than the average employee, he might understand that you can change the extension of the file name to disguise it. Thus, "vacationplans.doc" might be renamed "plans.dll." A cursory look at the file name would lead you to ignore the file as some type of system file. If you looked at the file in Windows Explorer you would find the icon was changed and you would no longer see the typical Microsoft Word icon next to the file name. The employee would know that if he wanted access to the file he would only need to rename the file and change the extension back to the original. Using forensic software, however, this attempt to hide the document would easily be discovered. Every file type has standard header information as part of its metadata that is unrelated to the extension or the icon that appears in Windows Explorer. The forensic software can be used to identify all files by type, and this will enable the examiner to show that the file named "plans.dll" was in fact a Microsoft Word document that is a copy of a proprietary memo that was originally found on the employer's network. Again, this is evidence of culpable conduct which is even stronger than the mere existence of a file on the local hard drive or the fact that it is hidden in a series of nested folders and renamed. You might be able to explain away that fact you "accidentally" made a copy of a file to your local computer, but if you rename it and change the extension you would be hard pressed to claim this was an innocent act.

Assume after the employee decided to steal information, and as part of the planning process, he created shortcuts on his desktop to key documents on the corporate network. He wanted to be sure he could find the documents quickly when it came time to copying them to a thumb drive. These links will be identified during the course of a forensic examination. Even if the employee copied the files to a thumb drive, and not to the actual hard drive of the employee's computer, the links will remain; and they will point to the location on the employer's network where the original files reside. Thus, the presence of the link files when looked at in conjunction with the source files on the network server will serve as evidence that the employee had targeted these key files.

The lawyer should be told that if the files were copied to a thumb drive, there is additional information that can be found in a forensic examination that will corroborate the fact that a thumb drive was attached to the employee's computer. A registry analysis will identify every external device that was attached to the computer by the date the device was connected, the time the device was connected, and the name and serial number of the device that was connected. It won't tell you who was on the computer at the time or which files were copied, but it will provide some evidence that can be followed up in further discovery that can establish the theft.

In a typical situation it's common that external memory devices were attached the day or night before the employee quit, which by itself is circumstantially

suspect. It is useful evidence to include in an affidavit or in testimony in support of a motion for a temporary restraining order. The registry analysis will provide the necessary information to identify the devices that were attached, and requests for production of these devices to the employee can follow in the course of further discovery. An expedited order to produce could be obtained as part of the requested injunctive relief, and if upon forensic examination of the thumb drive the suspect files are found you've established employee theft.

A registry analysis can also provide evidence of suspect software being installed and then uninstalled. Someone who wants to copy large volumes of information may simply want to copy the entire hard drive. This is particularly true if the employee uses a laptop. They are more likely to keep local copies of key information on a laptop. Since they can take the laptop off site they may be tempted to simply copy the entire hard drive to an external drive or another computer using software like Norton Ghost. They may try to cover their tracks by using software like EvidenceEliminator or Evidence-Blaster. While they may succeed in overwriting deleted data making the deleted files unrecoverable, the fact that they installed and then uninstalled evidence wiping software a day or two before they quit will remain in the registry. This raises the interesting question of what type of evidence is worse, the forensic recovery of deleted files showing proprietary information was on the employee's computer but deleted, or the presence of unauthorized evidence elimination software that could only be present for the purpose of spoiling the evidence. If you are lucky you may get both.

The attorney should be advised that another common way to steal information is to e-mail it as an attachment. Some employees are foolish enough while using their work account to e-mail documents directly to a personal e-mail account. Others may think that by sending the information to a legitimate recipient, while blind carbon copying their personal e-mail address, they will hide the fact they've transmitted something to themselves. Since experience shows that employees will do this, the e-mail server and any e-mail related evidence that remains on the employee's computer should be examined. More often the employee thinks that by using web-based e-mail they can avoid detection. They sign on to a Hotmail or Yahoo account and forward information home thinking no one at work will ever know what they did. Using the Internet, however, leaves forensic tracks and an Internet usage analysis will disclose the use of web based e-mail, information about the e-mail, the names of the files that were attached, and possibly cached copies of the attachments if they were opened in the browser for review before sending.

Some employees don't understand that deleting a file, or even emptying the recycle bin, does not mean a computer file cannot be recovered. Be sure to explain that unless the original data has been overwritten with new data, a file

can be recovered using forensic software tools. Thus, another important aspect of a forensic examination is the examination of deleted but recoverable files. In many instances the entire file can be recovered. In some cases only portions of a file can be recovered. However, even file fragments provide information about the original file. Employees who copy information from the network to their local hard drive, then copy files in bulk to a removable storage device, and then delete the files on their local computer, have not eliminated evidence of what they have done. By restoring the files you can determine from the metadata when they were originally created, when they were last modified, and when they were last accessed.

In addition, given that each file has an individual hash value, and assuming the files were not modified in any way that would alter the hash value, it is possible to correlate the deleted information with the original files on the network server and on the computer or external drive to which they were copied.

Finally, don't forget that in this day and age of telecommuting employees, home computers may be a rich source of evidence. Advise the attorney that a preservation letter followed by a motion seeking an order requiring preservation should be issued immediately. In many cases, particularly if insufficient evidence is obtained by analyzing the work computers, an analysis of the home computer is warranted. Evidence pointing to the use of home computers can be obtained by reviewing network logs indicating the dates and amount of time an employee was connected to the employer's network. If the dates are suspicious or the amount of time connected seems suspect, a legitimate basis to compel production of the home computer can be made.

There is much more that a forensic examination of a departed employee's computer can disclose, but the foregoing examples give a good idea of the types of information that can typically be obtained through computer forensics. The vast majority of attorneys don't have this basic knowledge and they need to be educated. They need to be shown that early analysis of ESI can give them much more evidence to use when seeking injunctive relief. Because electronic data is by nature volatile, preservation concerns must be at the top of your list when working with an attorney on a new employee theft case. Explaining what you can get through early computer forensic analysis and e-Discovery should help you and the attorney understand the issues and take the necessary preliminary steps to build a strong case—one strong enough to support a winning motion for a temporary restraining order.

Bruce A. Olson is President of ONLAW Trial Technologies, LLC, a consulting firm offering trial technology, e-Discovery, and computer forensics services. Previously, he was a shareholder in the Milwaukee-based law firm of Davis & Kuelthau, s.c. A trial attorney and nationally recognized legal technologist, Olson

is AV rated and Board Certified by the National Board of Trial Advocacy. He is co-author of "The Electronic Evidence and Discovery Handbook: Forms, Checklists and Guidelines," published by the American Bar Association. He received the prestigious TechnoLawyer of the Year 2002 @Award form TechnoLawyer, and was Chair of ABA TECHSHOW 2004, Vice Chair of ABA TECHSHOW 2003, and served on the TECHSHOW Board of Directors from 2000-2004. He can be contacted at (920) 750-8083 or bolson@onlawtec.com.

Entrepreneurial Espionage – Made in China

http://blogs.forbes.com/williampentland/2011/01/22/entrepreneurial-espionage-made-in-china/

Jan. 22 2011 - 8:23 pm

By WILLIAM PENTLAND

China's President Hu Jintao promoted the emerging spirit of American-style entrepreneurialism during his visit to Washington D.C. this week for the highly-scripted U.S.-China Summit.

Jintao has not yet commented on the status of Chinese government's home-grown brand of "shadow innovation," which began nearly 30 years ago and is evolving today into an insidious and dangerous trend called "entrepreneurial espionage."

In 1986, Deng Xiao Peng established "Program 863," a sort of academy of sciences and technologies charged with closing the scientific gap between China and the world's advanced economies in a very short period of time. The 863 program and its institutional derivatives not only sponsored actual research, they also promoted the acquisition of advanced technologies from other countries legally or illegally.

Today, counter-intelligence activities in the United States that have a nexus with China typically involve the illegal acquisition of U.S. technologies. Unlike Russian intelligence officers looking to exploit ego, greed, or other personal weaknesses, China has not normally paid agents for classified documents or engaged in clandestine activity like 'dead drops.'

While some of the recent espionage cases brought against China have ties to China's intelligence services, the vast majority are linked to other state organizations, particularly the factories and research institutes of China's military-industrial complex. Multiple Chinese state entities are engaged in an active effort

to acquire restricted U.S. technologies. Unlike other foreign governments, China has a history of encouraging and rewarding private individuals to obtain technology on its behalf.

Chinese intelligence practices rely on nonprofessional collectors motivated by profit, patriotism or other factors and acting either independently or on behalf of the Chinese government to gather science and technology intelligence. Nonprofessional intelligence collectors—including government and commercial researchers, students, academics, scientists, business people, delegations, and visitors—also provide China with a significant amount of sensitive U.S. technologies and trade secrets," according to reports by the Office of the Director of National Intelligence. "[I]n many cases, the collection efforts of these private-sector players are driven entirely by the opportunity for commercial or professional gain and have no affiliation with [PRC intelligence]."

This practice has led to a vast amount of "entrepreneurial" economic and industrial espionage conducted by Chinese students, trade delegations, businessmen and educational and research institutions, according to reports by the U.S.-China Economic And Security Review Commission.

The Chinese government encourages such efforts and has benefited from them.

In 2009, the Commission quoted testimony provided by former FBI Special Agent I.C. Smith that the Ministry of State Security sometimes places pressure on Chinese citizens going abroad for educational or business purposes and may make pursuit of foreign technology a quid pro quo for permission to travel abroad. However, this phenomenon of "entrepreneurial espionage" appears to be particularly common among businessmen who have direct commercial ties with Chinese companies and who seek to skirt U.S. export control and economic espionage laws in order to export controlled technologies to the PRC. In such instances, profit appears to be a primary motive, although the desire to"help China" can intersect in many cases with the expectation of personal financial gain.

"Espionage entrepreneurs" are not focused solely on obtaining state-of-the-art, high-tech data and equipment. In many cases there is no obvious direct state involvement in the theft or illegal export of controlled technology. These entrepreneurial efforts frequently take the form of "mom-and-pop" companies—many of them nothing more than a titular business registered at a residential address—that legally purchase older military technology from U.S. manufacturers or through a secondary market of defense industrial equipment auctions, or even from the Internet, and then look for customer institutions back in China.

"There are pieces of technology . . . that the Chinese are trying to acquire that are 20, 25 years old, [and] that are mainstays of existing U.S. defense systems but come nowhere close to being considered state-of-the-art, and yet a means-ends test would correctly identify those as critical gaps in the Chinese system," said Dr. James Mulvenon, a specialist on the Chinese military at the Defense Group, Inc., stated during testimony before the Commission in 2009.

Corporate spying in India: The tools they use

http://www.rediff.com/business/slide-show/slide-show-1-corporate-spying-a-booming-business-in-india/20110517.htm?print=true

Last updated on: May 17, 2011 11:40 IST

There is no business booming more in India than corporate espionage. According to industry estimates, private detective agencies receive more than 10 requests a day by companies to spy on their rivals.

Fees for such services can range from Rs 50,000 to several lakhs of rupees. With the competition increasing in the corporate world, companies are using every trick in the book to position their brand, launch new products and retain the best people.

A recent survey conducted by consultancy firm KPMG showed that 14 per cent of Indian companies have been victims of corporate spying.

Analysts say the actual figure is certainly higher than this as many companies do not report cases of intellectual theft or spying because they are afraid that going public might hurt their image and balance sheet.

Although everybody admits that corporate espionage is a growing problem, few are willing to go to court.

Experts say one reason could be the issue with Indian lax laws on spying and intellectual theft, firms do not see much benefit in spending money and time on legal action when successful prosecution could take years.

Legal analysts, on the other hand, cite the successful and timely settlement of Purolite-Thermax case as evidence that companies should not shy away from either going public or taking legal action.

In early 2011, an Indian company -- Thermax -- agreed to pay United States-based Purolite $38 million to settle a case over alleged unauthorised usage of water purification technology.

Hacking

Hacking is one of the most favourite tools of anyone trying to gain access to secret information.

There are three types of hacking: Remote, systems and physical.

Remote hacking is when an attacker enters the network remotely and without any special privileges. After securing access to administrative or higher level, the hacker steals the confidential information.

System hacking is when an attacker, who already has access to low-level or privilege user account, exploits a security issue or a hole in security settings to gain access to secret information.

Physical hacking is when an attacker personally enters a building and tries to gain information through unsecure workstations, servers or telephone room. Hacking has become the preferred method because of easy availability of hacking tools and also because it is comparatively easy to do.

Social engineering

Social engineering is another preferred method of stealing classified information. Social engineering involves an attacker sending an email in the guise of a system administrator requesting the user's password for some maintenance work. The attacker will send the same email to several employees hoping that at least one unsuspecting employee will fall for the trap.

Password guessing in another technique. If an attacker can find out personal details about the target, such as children's name, birthdays, etc, he can most probably guess the password.

Garbage

Although rummaging through garbage sounds disgusting, it is one of the most successful methods to glean secret data.

People sift through trash to get their hands on such things as memos, printouts of sensitive data, company policy manuals, etc.

Wireless hacking

To gain access to wireless network, all an attacker needs is the correct radio and proximity to the network.

Once the intruder has the basic tools, he can access both wired and wireless networks.

Mobile phones

There are companies that provide devices to monitor a targeted phone's location, listen to phone calls via a web interface and check the user's text messages and web history.

Document Scanners

There are pen-like devices that can scan whole documents without anybody noticing anything.

Some of these devices come with 64MB of internal memory, take MicroSD cards for expansion and can perform Bluetooth transfers as well.

They can scan without a computer, are highly portable and can transfers files to a BlackBerry or Windows Mobile smartphone or a computer.

Remote monitoring equipment

There are tools that let you watch a live video feed from anywhere and listen in to phone conversations.

One such device is an 'air freshener' that has a colour camera inside, plus a SIM card that lets you watch the live video feed on a 3G phone.
There are also versions that call you when the device detects voices in a room.

It's the human threat, stupid

http://www.csoonline.com/article/print/682445

Eric O'Neill, the former FBI operative who played a crucial role in the arrest and conviction of FBI agent Robert Hanssen for spying against the U.S. for the former Soviet Union and Russia, says security can't rely on tech alone.

George V. Hulme, CSO

May 17, 2011

Anyone who has worked to defend enterprise secrets from theft knows that the answer to success certainly doesn't come from technology alone.

Few know this better than Eric O'Neill. O'Neill is the former FBI operative who worked as an investigative specialist and played a crucial role in the arrest and conviction of FBI agent Robert Hanssen for spying against the U.S. for the former Soviet Union and Russia. The 2007 movie "Breach" was based on O'Neill's experience investigating Hanssen.

"The human element is usually the weakest link," O'Neill said yesterday at the 2011 Computer Enterprise and Investigations Conference (CEIC) 2011.

That's not to say IT security isn't important. It is. In fact, the forensic analysis of a Palm Pilot played a crucial role in the apprehension of Hanssen, as it detailed the location and time of his next drop to the Russians. And the explosion of electronic devices has become crucial to fighting both the spying of nations and of corporate espionage. "Spies previously had to first photocopy or photograph the material they wanted, then make arrangements for drops and payments," O'Neill said. "Today they just capture it on their phone and email it to anywhere in the world."

It's also probably no surprise that an attacker today is likely to start their attack with their web browser. "When you think of hackers, the hackers will spend some time social engineering their targets rather than spend hours of hacking," he said. "If I were to try to steal from you, I would examine your personnel, and today I'd start on Twitter, Facebook, and look at as many people involved with you that I can find," O'Neill said. "I would look for people who talked about how they hated their boss. I'd find out where they like to hang out and I'd go see what they had to say," he said.

Some of the other things an attacker is likely to do to start, O'Neill said, is to comb through public Web sites, file Freedom of Information Act (FOIA) requests, eavesdrop on employees at airline terminals. "Be careful when traveling abroad, don't leave your laptop in hotel room," he said. "Dumpster diving is also one of the easiest ways to find out about someone."

Also, don't underestimate the depths an adversary might go to grab the information they seek. He told one story of an organization setting up a fake charity and requesting older computers be donated from the target company. "The company donated the computers to what they thought was a charity, and the drives had plenty of information on them," he said. "Front companies are a common technique," he said.

Another company sought to steal secrets from a U.S. company. This company played as if they were forming a partnership -- and said as part of an international relations building effort they were funding a documentary. They asked if they could send a film crew to the target company. "The targeted company was smart at first, and granted permission for a film crew of three.

Well, 10 people showed with cameras and started moving through the building. They lost track of many of them and they stole everything they wanted," he said. Also, don't think it's only large companies that are being targeted. "If I want to attack the State Department, am I going to approach the State Department directly, or am I going to approach a State Department contractor with much less security?" he asked. Of course, they're going to target the least defended entryway. That means smaller firms with larger -- or even interesting -- partners need to always be on the lookout for these potential threats themselves.

There's much at stake, O'Neill believes. "Information is the key to world leadership today. Attackers seek anything, from solar array technology to the next vaccine, that they think will help them get a head start on technological superiority," he said.

CYBER, HACKING, DATA THEFT, COMPUTER INTRUSIONS & RELATED

China Confirms Existence of Elite Cyber-Warfare Outfit the 'Blue Army'

http://www.foxnews.com/scitech/2011/05/26/china-confirms-existence-blue-army-elite-cyber-warfare-outfit/

Published May 26, 2011

China set up a specialized online "Blue Army" unit that it claims will protect the People's Liberation Army from outside attacks, prompting fears that the crack team was being used to infiltrate foreign governments' systems.

At a rare briefing, China's defense ministry spokesman, Geng Yansheng, announced that the 30-strong team was formed to improve the military's security, the Beijing News reported Thursday.

When a reporter asked if the Blue Army was set up in order to launch cyber attacks on other countries, Geng said that internet security was an international issue that impacted not only society but also the military field, adding that China

was also a victim of cyber attacks and that the country's network security was currently relatively weak.

The online unit, organized under the Guangdong Military Command, is believed to have existed for at least two years before Geng's acknowledgment Wednesday.

Sources throughout the internet security industry have long believed that China-based hackers are the single largest source of worldwide cyber attacks.
A report from US anti-virus software maker Symantec last year found that almost 30 percent of so-called malicious emails were sent from China, with 21.3 percent of the attacks originating from the eastern city of Shaoxing.

Social-Engineer Tool Review

http://www.social-engineer.org/newsletter/SocialEngineerNewsletterVol02Is20.htm

KeeDragon sent us a neat new device that Jim had a chance to review. The KeyDemon Wifi Keylogger will surely be an interesting device to be used in SE Audits - check out the review below:

When conducting a physical penetration test, one of the most useful sources of information can be a physical keystroke logger. However the biggest drawback to these are you not only have to gain enough access to install the logger, but you later have to return to retrieve it, this doubles your chances of getting caught.

An interesting approach to this problem however is a device that was sent to us for review, a USB keystroke logger that also has wifi access. Using the wifi network connectivity, it's able to e-mail the keystroke logs on a regular basis. The device itself is small, and looks like an extender of sorts. Not something that many people would take notice of, if they even looked at the back of their computer. As for the standard usage mode of the keylogger, there is not much to say. It works as needed. Plug it in, it starts logging keystrokes. Simple. To retrieve the logs, you simply plug it into your computer and hit a user defined keystroke (by default it is three letters on the keyboard at the same time) and

the device goes into "mass storage" mode, and acts just like a thumb drive. Now, when in thumb drive mode don't expect incredible performance, as its not the fastest drive you have ever seen, but it works for what is needed.

The other aspect of the mass storage mode is this allows you to configure the device. Options such as changing the keystroke for going into mass storage mode, the interval between time stamping the log, and so on. It is really simple, and not difficult to set up and use. Configuring the wifi is likewise just as easy, just editing another text file to define what SSID to connect too, any encryption, etc. Another important part here is defining the e-mail address that the logs should be sent to.

Other nice thing about the device is it has a little Windows GUI in case you are not comfortable editing text files directly. This little wizard style interface allows you to set up the various setting that you might need. It even works over a network as well, which in cases where you have another system on the same LAN could allow for on-demand retrieval of data.

Really, if you consider the damage that could be done with this sort of device over the long term, it is quite scary. Consider an executive assistant to a CEO getting this installed on his system. How log could it stay there capturing keystrokes before it is found? All the password changes, all the e-mail, web sites accessed, and so on. And when the device is discovered, then what? If they can figure out what the device is, and how to access it, they will get an e-mail address that the logs have been sent too.

Physical attacks such as this are often overlooked, but at the same time they can be some of the most devastating and effective social engineering attacks that can be leveraged against a company.

One word of caution however: Don't get ahead of yourself before using something like this on an engagement however, make sure your rules of engagement clearly dictate that this sort of compromise is allowed, and any exclusions that may be in place.

As powerful as this device is, it is not practical to use in all situations, especially with how common laptops have become. You really need a traditional desktop computer to target. Additionally, the SMTP sending of messages leaves something to be desired. If you don't manually set the SMTP server and allow it to just use the default server, it does not work as a connection is not able to be made.

So make sure you have access to a SMTP relay that will work before you try to make use of this feature. The instruction manual makes no mention of this, and

it's something that could really ruin your day if you don't have it tested out before hand.

Additionally, the network configuration features of the device worked very spotty in our testing, often being unable to identify the key logger over the network. Our recommendation is to use the direct configuration, and not worry about the over the LAN features until a software update is available.

Despite those drawbacks, this can be a very useful device in the context of a social engineering penetration test, and one worth checking out. If you find this interesting, you might want to check out some of the other devices they sell, including a similar device that will capture video snapshots on a user defined interval.

10 Cybersecuriy Tips for Small Business

http://transition.fcc.gov/Daily_Releases/Daily_Business/2011/db0516/DOC-306595A1.pdf

Broadband and information technology are powerful factors in small businesses reaching new markets and increasing productivity and efficiency. However, businesses need cybersecurity tools and tactics to protect themselves, their customers, and their data from growing cyber threats. Here are ten key cybersecurity tips for businesses to protect themselves:

1. Train employees in security principles

Establish basic security practices to protect sensitive business information and communicate them to all employees on a regular basis. Establish rules of behavior describing how to handle and protect customer information and other vital data. Clearly detail the penalties for violating business cybersecurity policies.

2. Protect information, computers and networks from viruses, spyware and other malicious code Install, use and regularly update antivirus and antispyware software on every computer used in your business. Such software is readily available online from a variety of vendors. Most software packages now offer subscriptions to "security service" applications, which provide additional layers of protection. Set the antivirus software to automatically check for updates at a scheduled time of low computer usage, such as at night (midnight, for example), and then set the software to do a scan after the software update.

3. Provide firewall security for your Internet connection

A firewall is set of related programs that prevent outsiders from accessing data on a private network. Install and maintain firewalls between your internal network and the Internet. If employees work from home, ensure that their home systems are protected by firewalls. Install firewalls on all computers – including laptops – used in conducting your business.

4. Download and install software updates for your operating systems and applications as they become available All operating system vendors regularly provide patches and updates to their products to correct security problems and improve functionality. Configure all software to install such updates automatically.

5. Make backup copies of important business data and information.
Regularly backup the data on every computer used in your business. Critical data includes word processing documents, electronic spreadsheets, databases, financial files, human resources files and accounts receivable/payable files. Backup data automatically if possible, or at least weekly.

6. Control physical access to your computers and network components
Prevent access or use of business computers by unauthorized individuals. Laptops can be particularly easy targets for theft, so make sure they are stored and locked up when unattended.

7. Secure your Wi-Fi networks
If you have a Wi-Fi network for your workplace make sure it is secure and hidden. To hide your Wi-Fi network, set-up your wireless access point or router so it does not broadcast the network name, known as the Service Set Identifier (SSID). In addition, make sure to turn on the encryption so that passwords are required for access. Lastly, it is critical to change the administrative password that was on the device when it was first purchased.

8. Require individual user accounts for each employee
Setup a separate account for each individual and require that strong passwords be used for each account. Administrative privileges should only be given to trusted IT staff and key personnel.

9. Limit employee access to data and information, and limit authority to install software

Do not provide any one employee with access to all data systems. Employees should only be given access to the specific data systems that they need for their jobs, and should not be able to install any software without permission.

10. Regularly change passwords

Passwords that stay the same, will, over time, be shared and become common knowledge to coworkers and can be easily hacked. Passwords should be changed at least every three months.

The FCC's Cybersecurity Hub at www.fcc.gov/cyberforsmallbiz has more information, including links to free and low-cost security tools.

Hackers Broaden Their Attacks

http://online.wsj.com/article/SB10001424052702304563104576355623894502788.html#printMode

Lockheed and PBS Join the Roster of Recent Victims as Motives Expand; 'Almost Anyone Is a Target'

By BEN WORTHEN, RUSSELL ADAMS, NATHAN HODGE and EVAN RAMSTAD

Hacking incidents at defense contractor Lockheed Martin Corp. and broadcaster PBS that surfaced over the past few days show how widespread corporate breaches have become and underline how any organization can become a victim. Over the weekend, the website for the PBS show "NewsHour" was altered by hackers to include a fake article claiming that rapper Tupac Shakur, who was murdered 15 years ago, was alive in New Zealand. The hackers also posted login information that stations and other entities use to access PBS sites.

The incident followed a recent breach at Lockheed, which said Saturday evening that it had detected a "significant and tenacious attack" against its computer networks on May 21. The company said it stopped the attack before data could be stolen.

The attacks are the latest in a mushrooming of breaches world-wide. While hackers once generally had targeted companies that stored financial data or had classified government information, culprits today are expanding their sights to other corporate secrets or seeking information that can lead to valuable data down the line. Amateur hackers also are becoming increasingly brazen.

In recent months, hackers stole data from EMC Corp.'s RSA security unit, email marketer Epsilon Data Management LLC, two of South Korea's largest banks and Sony Corp., where the breach temporarily hobbled its online PlayStation Network.

"Almost anyone is a target," said Alex Stamos, chief technology officer at security firm iSEC Partners. Professional hackers now "have good tools and good

technique and know how to string them together," he said. Hackers also are getting better at identifying the soft spots in corporate defenses, he said.

So-called hactivists, who take revenge on companies for perceived slights, also have moved from simply knocking websites offline to stealing data. "There are enough people out there who aren't worried about the consequences that they are willing to wage a sustained campaign against a global company," Mr. Stamos said.

Corporate executives said they no longer can take a passive approach to cybersecurity. Ted Chung chief executive of Hyundai Card/Hyundai Capital Co., an auto finance provider in South Korea that was hacked in April, blamed himself for not paying enough attention to the importance of information-technology security.

"When it comes to big companies or big banks, no CEO is that stupid not to pay attention. But maybe they pay the same attention I did, which is giving encouragement and budget to IT but then saying 'What do I know about programming?' "he said in an interview Monday."That is the wrong support."

The latest attacks demonstrate a diversity of motives. Those who attacked Hyundai Capital tried to extract ransom for a database they stole. With Epsilon, the hackers made off with email addresses that could be used to send "phishing" emails that trick recipients into disclosing personal information.

At RSA, the perpetrators stole data about security systems that the company sells to its clients. Alone, the data are worthless, security experts said, but they could be used to crack defenses used by other companies.

With PBS, a group identifying itself as LulzSec claimed credit for the fake article on Tupac Shakur, which the group said was retaliation for a documentary, "WikiSecrets," about the publication of classified documents on the WikiLeaks website and the Army intelligence analyst who has been charged with leaking them. "By the way, #WikiSecrets s—," a message to PBS said. While the attack was more akin to graffiti than burglary, it underscored the threats companies now face.

PBS on Monday said it had corrected the false information on its website and was "notifying stations and affected parties to advise them of the situation." The fake article first appeared late Sunday night on the PBS "NewsHour" news blog, "The Rundown." The group then posted a string of Twitter messages in which it took credit for the breach, beginning with a post that read, "Oh s—, what happened to @PBS?" followed shortly after by the post, "What's wrong with @PBS…? How come their database is seized? Why are passwords cracked? :(."

The group then posted links to pages with the login information for the PBS sites.

Shortly after the story was published, PBS "NewsHour" posted several messages on Twitter stating that the article wasn't produced by PBS and that the site had been hacked.

Separately, Lockheed said Saturday evening that the company's information-security team detected its attack "almost immediately and took aggressive actions to protect all systems and data."

"Our systems remain secure; no customer, program or employee personal data has been compromised," the company said. Lockheed said it was conducting an investigation and that it "has continued to keep the appropriate U.S. government agencies informed of our actions."

White House Press Secretary Jay Carney told reporters Sunday that President Barack Obama had been briefed on Lockheed attack and that the damage was understood as "fairly minimal."

Still, that attack is likely to ripple throughout the defense industry. Lockheed supplies some of the most sophisticated weaponry to the U.S. military and is a major provider of information technology to the federal government. The company, based in Bethesda, Md., also is a top international supplier of military and security hardware, employing around 126,000 people world-wide.

Speculation around the Lockheed attack centered on whether hackers may have breached the system by exploiting a vulnerability in SecurID electronic keys made by RSA. In a memo to employees on Sunday, Lockheed Chief Information Officer Sondra Barbour said the company "took swift and deliberate actions" to step up security, including shutting down a virtual private network, resetting user passwords and upgrading SecurID tokens, among other measures.

In South Korea, prosecutors believe North Korea was behind an attack on a large farm cooperative, which couldn't provide ATM, credit-card and online services for nearly a week after a system at its Seoul headquarters was accessed remotely. How law enforcement tracked the attack to North Korea wasn't disclosed. But authorities said a link was made to the same Internet servers North Korea used in a 2010 denial-of-service attack against South Korean government websites. North Korea called the South's accusation in the latest case "absurd" and "unreasonable."

At Hyundai Capital, a pair of hackers in South Korea gained access to the company's databases and downloaded personal information on 1.7 million

customers. After the company contacted police, it agreed to pay part of what hackers sought. Police arrested the hackers after one was recorded by an ATM video camera as the hacker tried to withdraw some of the ransom. The company has since revamped its IT operation and begun an overhaul of its cybersecurity.

—Ian Sherr contributed to this article.

Write to Ben Worthen at ben.worthen@wsj.com, Russell Adams at russell.adams@wsj.com and Evan Ramstad at evan.ramstad@wsj.com
Read more:
http://online.wsj.com/article/SB10001424052702304563104576355623894502788.html#ixzz1NwVWfYvB

Cloud Can Rain Down Malware, Hijacking, ID Theft, Data Loss, Piracy, Trojan Horses

http://www.hollywoodtoday.net/2011/05/05/cloud-can-rain-down-malware-hijacking-id-theft-data-loss-piracy-trojan-horses/

May 5th, 2011

Raindrops keep falling on my head...

Commentary by Erick Hansen

HOLLYWOOD, CA (Hollywood Today) 5/5/11 – Cloud Computing may rain on your parade. The latest buzz word in the online universe could soon become the most hated as the Cloud blows away to reveal such a potential major security storm that it makes present Internet problems look like a drizzle.

Cloud Computing refers to the largest Internet and computer companies as well as indies storing your life. The idea is to put all your data, such as credit info, personal and legal documents, family photos, even phone records in shared networks.

In exchange, you can use a dumb terminal and let the corporations handle it all. That would save you money on hardware, though in the era of laptops starting at $200, it is not clear how much you would save.

It could be dust in the wind and a waste of your money. While some people have their head in the clouds, others prefer their technology and personal info closer to the ground – and private.

Cloud technology may make Sony's loss of the data from 75 million accounts seem like just a breeze compared to what could happen if billions of users adopt the upcoming Cloud storm.

Cloud leaders like big brothers Cisco, Dell and Microsoft could be responsible for one of the biggest tech flops ever.

What if it is a sunny day and your cloud company has gone out of business? Or even if you cannot connect. When on the road your crucial data will be unavailable whenever your (expensive) mobile Internet does not work. Even in town, think about how many dropped calls you get on your regular cell phone. Both the Cloud dumb terminal and the connection need to work together to get "Dumb and Dumber."

The danger is waking up one bright day and having to ask "where is my money, personal info and family photos?"

They tried dumb terminals in the early days of personal computing, mainly just a keyboard and screen – with various networks handling your data and software. Turned out people liked to keep their personal info personal and the PC and Mac era began in earnest.

Even HP and the Cloud Security Alliance (CSA) have dire concerns over the potential threats hovering above the clouds – and they both want Cloud to succeed.

They both have published info on the Seven Deadly Sins of Cloud security.

The first is "Abuse and Nefarious Use of Cloud Computing:"

- Insecure Application Programming Interfaces
- Malicious Insiders
- Shared Technology Vulnerabilities
- Data Loss/Leakage
- Account, Service & Traffic Hijacking

The Cloud providers offer their customers the illusion of unlimited compute, network, and storage capacity — often coupled with a 'frictionless' registration process where anyone with a valid credit card can register and immediately begin using cloud services. Some providers even offer free limited trial periods.

By abusing the relative anonymity behind these registration and usage models, spammers, malicious code authors, and other criminals have been able to conduct their activities with relative impunity. Providers have traditionally

suffered most from this kind of attacks; however, recent evidence shows that hackers have begun to target IaaS vendors as well. Future areas of concern include password and key cracking, launching dynamic attack points, hosting malicious data, botnet command and control, building rainbow tables, and

CAPTCHA solving farms.

Impact

Criminals continue to leverage new technologies to improve their reach, avoid detection, and improve the effectiveness of their activities. Cloud Computing providers are actively being targeted, partially because their relatively weak registration systems facilitate anonymity, and providers' fraud detection capabilities are limited.

Another treat is that Cloud Computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. Provisioning, management, orchestration, and monitoring are all performed using these interfaces. The security and availability of general cloud services is dependent upon the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy.

Furthermore, organizations and third parties often build upon these interfaces to offer value-added services to their customers. This introduces the complexity of the new layered API; it also increases risk, as organizations may be required to relinquish their credentials to third parties in order to enable their agency.

Malicious Insiders

Description

The threat of a malicious insider is well-known to most organizations. This threat is amplified for consumers of cloud services by the convergence of IT services and customers under a single management domain, combined with a general lack of transparency into provider process and procedure. For example, a provider may not reveal how it grants employees access to physical and virtual assets, how it monitors these employees, or how it analyzes and reports on policy compliance.

To complicate matters, there is often little or no visibility into the hiring standards and practices for cloud employees. This kind of situation clearly creates an attractive opportunity for an adversary — ranging from the hobbyist

hacker, to organized crime, to corporate espionage, or even nation-state sponsored intrusion. The level of access granted could enable such an adversary to harvest confidential data or gain complete control over the cloud services with little or no risk of detection.

There are more threats documented at cloudsecurityalliance.org. Thank goodness most of us like to keep our info to ourselves, one hacker or virus here can infect a country.

Even now, about 69 percent of us (nearly 2 billion internet users) are using a type of Cloud such as your email service, which stores your email on its site until you delete it or reach a limit.

Yet you don't let them control your whole online and computing life. Disruption to Amazon.com Inc servers that host Internet services took down a raft of social networking websites including Foursquare and Quora early on Thursday, underscoring concerns about reliability as more companies turn to the "cloud."

Amazon's "Elastic Compute Cloud," part of the online retail company's cloud-computing service that hosts websites for startups, experienced latency problems and other errors, according to Amazon's status page.

The company said it was dealing with capacity issues amid a flood of queries and information, according to Reuters.

Amazon is "now seeing significantly reduced failures and latency and … continuing to recover. We have also brought additional capacity online in the affected availability zone," it said.

Now here's how one hacked can infect a planet. The video link to Microsoft's explanation of a global supercloud is chilling and spooky, though it is supposed to promote the Cloud.

http://www.microsoft.com/en-us/cloud/default.aspx?WT.srch=1&WT.mc_id=AEBF120C-9AC0-4DA4-B151-D9B6E31754CA&CR_SCC=200010704&fbid=KtimvU06aO5

Americans like their privacy and freedom and there are big questions on whether Cloud computing offers either. This writer believes Big Brother should blow away home and let us keep our personal data to ourselves and share it as we please, not as they do. Let the sun shine.

JUNE IN COUNTERINTELLIGENCE HISTORY

- June 3, 1957: On this date cryptanalysts at the FBI Laboratory decoded the message hidden in Soviet Spy Colonel Rudolph Abel's "hollow nickel", a device designed to conceal and contain coded messages, microdots and similar contraband. This story is one of the cases Jimmy Stewart solved in 1959's movie "THE FBI STORY".
- June 5, 1940: On this date a delimitations agreement was read between the FBI, the Office of Naval Intelligence and the Military Intelligence Department establishing the FBI as the primary entity responsible for domestic security.
- June 6, 1945: On this date the FBI arrested six individuals for conspiracy to violate the federal espionage statutes and unauthorized possession of classified documents. Government employees Emmanuel Larson and John Stewart Service were arrested, as were the editors of Amerasia, a left wing journal on Far East policy. Ultimately, there were no successful prosecutions associated with this case, due to the improper search and seizure of Amerasia's premises by FBI and OSS agents.
- June 9, 1950: Harry Gold, one of the so called "Atom Bomb Spies" was indicted on this date for conspiring to violate the Espionage Act of 1917.
- June 10, 1933: The Yardley Act, the Act for the Protection of Government Records, is established. Herbert Yardley, author of "THE AMERICAN BLACK CHAMBER", a best seller of the day, was a former codebreaker for the U.S. Government. When the Secretary of State famously stated that "Gentlemen do not read other gentlemen's mail…" and shut down the U.S. Government's highly successful codebreaking operations, Yardley wrote his best seller. "THE AMERICAN BLACK CHAMBER" detailed the numerous successes of the State Departments codebreakers, addressing the lives saved, enemy actions disrupted, and diplomatic victories achieved because of our skilled codebreakers.
- June 12, 1942: Four German saboteurs landed on the beach near Amagansett, Long Island, New York. Four others landed at Ponte Verda Beach, Florida on June 19, 1942. With the help of one of these saboteurs, the FBI had located and arrested all eight of the saboteurs by June 26, 1942.
- June 15, 1917: The Espionage Act of 1917 passed Congress.
- June 19, 1953: Julius and Ethel Rosenberg were executed on this date for passing American nuclear secrets to the Russians.
- June 21, 1957: On this date Russian illegal agent Colonel Rudolph Abel (see June 3, 1957 above) was arrested by the FBI in New York City.
- June 24, 1940: By Presidential Directive, the FBI's Special Intelligence Service is established and given the mission to gather intelligence throughout the Western Hemisphere.

- June 26, 1939: On this date, President Roosevelt issued a confidential directive to his Cabinet. The directive stated that all espionage, counterespionage, and sabotage matters were to be investigated by the FBI, the Intelligence Division of the War Department and the U.S. Navy.
- June 28, 1941: After a two year investigation, the FBI arrested 33 members of the Duquesne Spy Ring. Led by German spy Frederick Duquesne, the FBI filmed members of the spy ring providing information to a confidential informant.

PRESENTATIONS AND OUTREACH

The CI Strategic Partnership Newsletter is a product of the FBI's Counterintelligence Program Coordination Section which plays a key role in protecting our sensitive technologies from our adversaries.

The Challenge: to protect United States sensitive information, technologies and thereby competitiveness in an age of globalization.

Our Solution: to foster communication and build awareness through partnerships with key public and private entities, by educating, and enabling our partners to identify what is at counterintelligence risk and how to protect it. We call it "knowing your domain"—identifying the research, information and technologies that are targeted by our adversaries, and establishing an ongoing dialog and information exchange with partners, the goal of which is to change behaviors and reduce opportunities that benefit the opposition's efforts.

The United States is a world's leader in innovation. Consider the breakthrough research and development that's taking place on the nation's campuses and in research facilities—often on behalf of the government. Sensitive research, much of which occurs in the unclassified realm, is the key to our nation's global advantage, both economically and militarily.

The Counterintelligence (CI) Program Coordination Section is responsible for determining and safeguarding those technologies which, if compromised, would result in catastrophic losses to national security. Through our partnerships with businesses, academia, and US Government agencies, the FBI and its counterintelligence community partners are able to identify and effectively protect projects of great importance to the U.S. Government. This provides the first line of defense inside facilities where research and development occurs and where intelligence services are focused.

The FBI's outreach efforts continue to evolve. This newsletter is one way we hope to expand our outreach to the elements of our "CI Domain." We continue in contacting businesses and organizations with which we have not yet made personal contact. In support of its Counterintelligence Domain/Strategic Partnership Program, the Federal Bureau of Investigation hosts an annual Research and Technology Protection (RTP) Conference for Facility Security Officers and RTP Professionals. Unclassified presentations address specific country threats to your technology, industrial and economic espionage, counterintelligence threat issues, and computer intrusion/cyber threat matters. The annual RTP Conference is offered in two locations during the year: Orlando and Clearwater.

The FBI's Domain/Strategic Partnership Program seeks to interface with private industry, high tech companies, research institutes, any stakeholder and/or contractor that design, develop, produce, and distribute critical information and technologies. Our job is to establish contact with these "Domain entities" in our territory, and assist them to better understand the foreign intelligence threat, and improve their ability to institute protective mechanisms. In addition to hosting an annual Research Technology Protection (RTP) Conference for security professionals, we also provide security awareness threat briefings to our defense contractor partners, high tech companies and research institutes. To schedule CI, cyber, security, education, training and awareness briefings, contact the Tampa Domain/SPC.

The Tampa Field Office Counterintelligence Strategic Partnership Program Coordinator:

James "Pat" Laflin (James.Laflin@ic.fbi.gov) 813.253.1029

Federal Bureau of Investigation

5525 West Gray Street
Tampa, FL 33609
Phone: 813.253.1000