FBI Tampa CI STRATEGIC PARTNERSHIP NEWSLETTER

March 1, 2011
Volume 3 Issue 3

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

INSIDE THIS ISSUE:

COUNTERINTELLIGENCE (CI) TRENDS

A FEW TRENDS, CONGRESSIONAL TESTIMONY AND ITEMS OF INTEREST

REQUESTS TO ACCESS COMPUTERS BY STRANGERS AT THE AIRPORT

We want readers of this newsletter to be aware of what appears to be some sort of collector trend by possible foreign nationals. The method of operation is to approach DEFENSE CONTRACTOR employees at the airport as they await their flights and ask to borrow their laptop so they can check their email. The foreign nationals are persistent at making their requests. Below are two reports from two employees of a DEFENSE CONTRACTOR. One incident was at LAX; the other at the Orlando International airport.

A DEFENSE CONTRACTOR employee traveled through LAX. An interesting thing happened while waiting for his next flight to depart. He was working on his DEFENSE CONTRACTOR lap top when he was approached by a Chinese woman and then a Russian male who both wanted to use his DEFENSE CONTRACTOR laptop to access their email accounts and were willing to pay to allow them to use his laptop to access the internet. When told "no" they questioned him on why not.

A DEFENSE CONTRACTOR employee traveled through Orlando International Airport. While sitting in the airport waiting for his flight a young gentleman of Middle Eastern descent and accent approached him while he was working on his computer offline. The young man requested to use the DEFENSE CONTRACTOR'S computer to access his e-mail. He was politely told no, and he said it would be only for a minute. Again he was told no, and that the computer was not on line. He moved on.

Both incidents were of a nature that these DEFENSE CONTRACTOR employees reported the incidents to their security departments. These incidents both merit reporting to the Defense Security Service and the FBI as Suspicious Contact Reports (SCRs) as required by the NISPOM.
Readers are reminded to be vigilant at airports and other public places when using laptop computers. Please be safe and have Bluetooth capability shut down. If using Wi-Fi, please be aware that the security of public Wi-Fi networks is lax, and your online access may be susceptible to hacking by others utilizing the same Wi-Fi connection.

If readers of this newsletter are aware of similar incidents, we would be interested in hearing your stories. Please contact your Counterintelligence Strategic Partnership Program contacts as listed on the first page of this publication.

CONGRESSIONAL TESTIMONY

On an annual basis the heads of the U.S. Intelligence Community appear before members of Congress and give what is referred to as the Annual World Wide Threat Briefing. We thought recipients of this newsletter might be interested in reading the prepared testimony given this year regarding Russia.

Russia

Last year was marked by significant improvements in US-Russian relations. Russia has demonstrated a willingness to cooperate on some top priorities that it shares with the United States, such as signing the New START Treaty, cooperating on transit and counternarcotics in Afghanistan, and pursuing the pressure track against Iran's nuclear program. Other encouraging signs include Russian interest in discussing missile defense (MD) cooperation with the United States and NATO, talks on modernizing the Conventional Armed Forces in Europe Treaty, and progress on Russian accession to the World Trade Organization (WTO).

At the same time, policy disagreements persist. Some Russian elites still express suspicion that MD is ultimately directed against Russia. Russia shows no willingness to discuss the status of—much less withdrawal of its troops from—South Ossetia and Abkhazia, contested territories inside Georgia's internationally-recognized borders.

Despite the fact that Russia has moved closer to membership in the WTO, some Russian officials and key lobbies have lingering doubts the move is in their interests.

Russia continues to influence domestic politics in other former Soviet republics, most recently in Belarus. Russia's concern is not with human rights or democracy but rather with the fact that Belarus's authoritarian leader Aleksandr Lukashenko routinely resists bending to its will. In Ukraine, Russian officials have been eager to engage and promote Russian interests through the Moscow-friendly government there.

The direction of Russian domestic politics is a major unsettled question for 2011 and 2012. President Medvedev's call for "modernization" has sparked a debate among the Moscow elite—and on the blogosphere—about whether

modernization is possible without political liberalization. Prime Minister Putin meanwhile has spoken forcefully against significant changes in the existing political order. In 2010, Russia saw a number of spontaneous protests, in part against unpopular government actions but also of a more nationalist bent. Opposition parties‟ popular support remains very weak.
The Russian economy has recovered from the 2008-2009 crisis and has returned to growth. However, the Russian leadership admits it will not repeat the rapid growth of the previous decade. The government has pledged to undertake new social programs and spend more on infrastructure and defense, which will challenge its ability to close the non-oil fiscal deficit.

The Russian Government is approaching the December 2011 Duma and March 2012 presidential elections having announced plans to increase resources devoted to address domestic problems and deal with the persistent security challenge in the North Caucasus. Popular and elite support for the existing political order appears strong enough to withstand these problems, at least in the short-term.

Putin and Medvedev indicate that the decision about who will be president hinges primarily on an arrangement between them. Both have shown interest in running.

Assessing Russia's Military

Russian military programs are driven largely by Moscow's perception that the United States and NATO are Russia's principal strategic challenges and greatest potential threat. Russia's nuclear forces support deterrence and enhance Moscow's geopolitical clout. Its still-significant conventional military capabilities, oriented toward Eastern Europe, the Caucasus, Central Asia, and the Far East, are intended to defend Russia's influence in these regions and serve as a "safety belt" from where Russian forces can stage a defense of Russian territory.

High-profile but small-scale operations in the Atlantic, Caribbean, Mediterranean, and Indian Ocean, in part, represent traditional peacetime uses of naval forces to "show the flag" and convey that Moscow remains a significant military power. Russia's ambitious military development plan announced in fall 2008 aims to field a smaller, more mobile, better trained, and modernized force over the next decade. This plan represents a radical break with historical Soviet approaches to manpower, force structuring, and training.

Moscow's military development poses both risks and opportunities for the United States and the West. Increased Russian capabilities and a strategy of asymmetric and rapid response raise the specter of a more aggressive Russian reaction to crises perceived to impinge on Moscow's vital interests. Moscow's wariness of the

potential for Western involvement on its periphery, concern about conflicts and their escalation, and military disadvantages exacerbated by a drawn out crisis or conflict place a premium on quick and decisive action. However, as the Russian military continues its post-Soviet recovery and Moscow feels more comfortable asserting itself internationally, Russian leaders may be more inclined to participate in international peacekeeping operations.

The Caucasus and Central Asia

The unresolved conflicts of the Caucasus and the fragility of some of the Central Asian states provide the most likely flashpoints in the Eurasia region. Moscow's continued military presence in and political-economic ties to Georgia' separatist regions of South Ossetia and Abkhazia, combined with Georgia' s dissatisfaction with the status quo, account for some of the tensions. Georgia' s public efforts to engage with various ethnic groups in the Russian North Caucasus have also contributed to these tensions.

Georgia's new Constitution strengthens the office of the Prime Minister after the 2013 presidential election. President Saakashvili has not indicated his future plans but the option is available for him under the new Constitution to serve as Prime Minister.

The frozen Nagorno-Karabakh conflict is also a potential flashpoint. The Azerbaijan government seems satisfied with the stalled Turkey-Armenia rapprochement, but President Aliyev is seeking to focus Western attention on Azerbaijani interests at the expense of Armenia. Heightened rhetoric and distrust on both sides and violent incidents along the Line of Contact throughout last summer increase the risk that minor military exchanges could lead to miscalculations that could escalate the situation with little warning.

As the US increases reliance on Central Asia to support operations in Afghanistan, the region's political and social stability is becoming more important. The overthrow of the Kyrgyzstani Government last April and the subsequent ethnic violence in the country's south attest that instability can come with little warning in parts of Central Asia. While Kyrgyzstan successfully held a parliamentary election, many underlying grievances have not been resolved and the possibility of episodic, retaliatory violence cannot be excluded. Kyrgyzstan's and Tajikistan's abilities to cope with the challenge of Islamic extremism—should it spread from Pakistan and Afghanistan—represent an additional cause for concern. In 2010, Tajikistan's President Rahmon was forced to negotiate with regional warlords after failing to defeat them militarily, an indicator that Dushanbe is potentially more vulnerable to an Islamic Movement of Uzbekistan with renewed interests in Central Asia.

As a part of the same World Wide Threat Briefing, Director of National Intelligence Clapper gave the following testimony captioned:
Intelligence Threats and Threats to US Technological & Economic Leadership

http://www.dni.gov/testimonies/20110210_testimony_clapper.pdf

Intelligence Threats

It is difficult to overstate the importance of counterintelligence to U.S. national security. The United States remains the highest priority intelligence target for many foreign intelligence services, and we continue to face a wide-range of foreign intelligence threats to our political, military, economic, and diplomatic interests at home and abroad.

In addition to the threat posed by state intelligence services, the intelligence capabilities and activities of non-state actors are increasing in scope and sophistication. And, the cyber environment provides unprecedented opportunities for adversaries to target the US due to our reliance on information systems. The spectrum of threats includes espionage, cyber intrusions, organized crime, and the unauthorized disclosure of sensitive and classified US Government information, a notable recent example being the unlawful release of classified US documents by WikiLeaks. While the impacts of the WikiLeaks disclosures are still being assessed, we are moving aggressively to respond by protecting our information networks with improved CI analysis of audit and access controls, improving our ability to detect and respond to insider threats—while balancing the need to share information—and increasing awareness across the U.S. Government to the persistent and wide ranging nature of foreign intelligence threats.

Far-Reaching Impact of the Cyber Threat

The national security of the United States, our economic prosperity, and the daily functioning of our government depend on a dynamic public and private information infrastructure. This infrastructure includes computer networks and systems, telecommunications and wireless networks and technologies that carry data and multimedia communications, along with control systems for our power, energy distribution, transportation, manufacturing, and other infrastructures. This information structure will also include new innovations such as the "Smart Grid" for intelligent production, distribution, and use of electric power.

We are also undergoing a phenomenon known as "convergence," which amplifies the opportunity for disruptive cyber attacks, including against physical

infrastructures. This phenomenon means that the same networks and devices are processing a full range of data and support a full range of applications, from banking to social networking, from supply chain management to patient health records. This convergence adds much convenience, but it poses new security challenges across a swath of our government and economy.

As we expand our ability to create and share knowledge, maintain our society and produce economic goods, we are developing new vulnerabilities and enabling those who would steal, corrupt, harm or destroy public and private assets vital to our national interests. In the past year, we have seen a dramatic increase in malicious cyber activity targeting US computers and networks; almost two-thirds of US firms report that they have been the victim of cybersecurity incidents or information breaches, while the volume of malicious software ("malware") on American networks more than tripled from 2009.

Industry estimates that the production of malware has reached its highest levels, with an average of 60,000 new pieces identified per day. Almost half of all US computers have been compromised, according to another industry survey. This current environment favors those who desire to exploit our vulnerabilities with the trend likely getting worse over the next five years because of the slow adoption of defensive best practices and rapid advances in offensive vulnerability discovery and exploitation.

In April a large number of routing paths to various Internet Protocol addresses were redirected through networks in China for 17 minutes due to inaccurate information posted by a Chinese Internet Service Provider. This diversion of data would have given the operators of the servers on those networks the ability to read, delete, or edit e-mail and other information sent along those paths. This incident affected traffic to and from U.S. Government and military sites, including sites for the Senate, the Army, the Navy, the Marine Corps, the Air Force, and the office of the Secretary of Defense, as well as a number of Fortune 500 firms. The complex, global nature of our information technology supply chain can hide many risks. Such vulnerability was demonstrated by employees at a US firm who were convicted for supplying counterfeit computer hardware to U.S. government, military, and private sector customers.

We are seeing a rise in intellectual property theft. Last year some of our largest information technology and defense contractor companies discovered that throughout much of 2009 they had been the targets of a systematic effort to penetrate their networks and acquire proprietary information. The intrusions attempted to gain access to and potentially modify the contents of source code repositories, the intellectual "crown jewels" of most of these companies.
Our identities are increasingly vulnerable. Cyber criminals are stalking prospective victims on social networking sites, acquiring personal information to

tailor "spear phishing" emails to gather more information that can be used to facilitate identity theft. They are intercepting messages exchanged by mobile devices to validate transactions, and masquerading as their victims to steal funds from their bank accounts. Further, the consolidation of data captured in emails, social networks, Internet search engines, and geographic location of mobile service subscribers increases the potential for identification and targeting of government personnel by criminals, or by intelligence organizations.

In the last year, we have witnessed the emergence of foreign military capabilities in cyber space. This formalization of military cyber capabilities creates another tool that foreign leaders may use to undermine critical infrastructures that were previously assumed secure before or during conflict. The IC is reaching out to the private sector to ensure current understanding of the dynamic cyber environment. More government-private sector and international cooperation is still required across the cybersecurity landscape.

In August, 2010, FBI Director Mueller addressed the International Conference on Cyber Security with the following remarks pertaining to the cyber threat:

http://www.fbi.gov/news/speeches/using-partnerships-to-combat-cyber-threats

Robert S. Mueller, III
Director
Federal Bureau of Investigation

International Conference on Cyber Security 2010 New York, New York
August 05, 2010

Good morning. It is a pleasure to be here. My thanks to Fordham University for hosting this conference and for co-sponsoring it with the FBI.

It is perhaps a little unusual to start a speech by pausing for five seconds, but that is what I would like to do.

What just happened? In those five seconds, computer users conducted some 170,000 Google searches. An estimated 22 million e-mails were sent—and about 80 percent of those were spam. Users posted at least 3,500 status updates on Facebook and 3,000 "tweets" on Twitter.

Meanwhile, the Automated Clearinghouse—the network that connects all U.S. financial institutions—processed almost 3,000 electronic payments. All of that happened in just five seconds.

We live in a wired world. Our networks help us to stay in touch with family and friends, collaborate with colleagues worldwide, and shop for everything from books to houses. They help us manage our finances and make businesses and government more efficient.

But our reliance on these networks also makes us vulnerable. Criminals can use the Internet to commit fraud and theft on a grand scale, and to prey upon our children. Spies and terrorists can exploit our networks to steal our secrets, attack our critical infrastructure, and threaten our national security. And because the web offers near-total anonymity, it is difficult to discern the identity, the motives, and the location of an intruder.

Yet for too many individuals and businesses, cyber crime remains a nebulous concept. So today, I want to talk about the evolving nature of cyber threats, what the FBI is doing to combat them, and how we can work together to keep them at bay.

Cyber Terrorism

Let me begin with cyber threats to our national security. As you well know, a cyber attack could have the same impact as a well-placed bomb.
To date, terrorists have not used the Internet to launch a full-scale cyber attack. But they have executed numerous denial-of-service attacks and defaced numerous websites.

In the past decade, al Qaeda's online presence has become almost as potent as its physical presence. Extremists are not limiting their use of the Internet to recruitment or radicalization; they are using it to incite terrorism.
Of course, the Internet is not only used to plan and execute attacks; it is also a target itself. Osama bin Laden long ago identified cyberspace as a means to damage both our economy and our morale—and countless extremists have taken this to heart.

We in the FBI, with our partners in the intelligence community, believe the cyber terrorism threat is real, and is rapidly expanding. Terrorists have shown a clear interest in pursuing hacking skills. And they will either train their own recruits or hire outsiders, with an eye toward coupling physical attacks with cyber attacks.
Apart from the terrorist threat, nation-states may use the Internet as a means of attack for political ends. Consider what took place in Estonia in 2007 and in the Republic of Georgia in 2008. Wave after wave of data requests shut down banks and emergency phone lines, gas stations and grocery stores, even parts of each country's government. The impact of these attacks left all of us aware of our vulnerabilities.

Counterintelligence and Economic Espionage
Let me turn for a moment to counterintelligence intrusions and economic espionage.

Espionage once pitted spy versus spy and country against country—as we have recently seen. Today, our adversaries sit on fiber optic cables and wi-fi networks, often unknown and undetected. They may be nation-state actors or mercenaries for hire, rogue hackers or transnational criminal syndicates.

These hackers actively target our government and corporate networks. They seek our technology, our intelligence, and our intellectual property, even our military weapons and strategies. In short, they have everything to gain, and we have a great deal to lose.

We are concerned not only about the loss of data, but corruption of that data as well. If hackers made subtle, undetected changes to your company's source code, they would have a permanent window into everything you do.
Some in the industry have likened this to "death by a thousand cuts." We are bleeding data, intellectual property, information, and source code—bit by bit, and in some cases, terabyte by terabyte.

The solution does not rest solely with better ways to detect and block intrusion attempts. We are playing the cyber equivalent of cat and mouse, and, unfortunately, the mouse seems to be one step ahead.

We must work to find those responsible. And we must make the cost of doing business more than they are willing to bear.

The FBI: Protecting Our Infrastructure

The FBI pursues cyber threats from start to finish. We have cyber squads in each of our 56 field offices around the country, with more than 1,000 specially trained agents, analysts, and digital forensic examiners.

Together, they run complex undercover operations and examine digital evidence. They share information with our law enforcement and intelligence partners. And they teach their counterparts—both at home and abroad—how best to investigate cyber threats.

But the FBI cannot do it alone. The National Cyber Investigative Joint Task Force includes 18 law enforcement and intelligence agencies, working side by side to identify key players and schemes. The goal is to predict and prevent that which is on the horizon, and to pursue the enterprises behind these attacks.

The task force operates through Threat Focus Cells—smaller groups of agents, officers, and analysts from different agencies, focused on particular threats. For example, the Botnet Focus Cell investigates high-priority botnets. We are reverse-engineering those botnets, with an eye toward disrupting them. And we are following the money wherever it leads, to find and stop the botmasters. The recent takedown of the Mariposa botnet is but one example of that collaboration. As you may know, Mariposa was an information-stealing botnet—one that infected millions of computers worldwide, from Fortune 500 companies to major banks.

During a two-year investigation, the FBI worked closely with our overseas counterparts to track down and arrest the main operators of the Mariposa botnet and the original creator of the malicious software that helped to build and control it.

In February, the Spanish police arrested three individuals who used Mariposa to hack into online bank accounts. And just two weeks ago, the Slovenian police identified and arrested the botnet's creator. This individual had sold the original virus to hundreds of criminals worldwide, and developed customized versions to meet their needs.

The Mariposa takedown sends a clear message to cyber criminals: We are going after both the cyber equivalent of the house burglar—and the person who gives him the crowbar, the map, and the locations of the best houses in the neighborhood.

The skill, dedication, and unprecedented cooperation provided by our partners in Spain and Slovenia were crucial to the success of this effort. In international cases such as this, global cooperation is absolutely essential.

To that end, the FBI has 61 legal attaché offices around the world, sharing information and coordinating investigations with our host countries. We have embedded agents with police forces in Romania, Estonia, Ukraine, and the Netherlands, to mention just a few.

Together, we are making progress. But law enforcement agencies alone cannot defeat our cyber adversaries. In the Mariposa case, our private sector partners also provided valuable help. The Mariposa Working Group, an informal band of security researchers and volunteers, gave us intelligence to track down the subjects, and worked to dismantle the botnet after we made our arrests.

Importance of Private Sector Partnerships

But to stem the rising tide of cyber crime and terrorism, we also need your help.

We in the FBI understand that those of you in the private sector have practical concerns about reporting breaches of your network security. You may believe that notifying the authorities will harm your competitive position. You may have privacy concerns. Or you may think that the information flows just one way—and that is to us.

We do not want you to feel victimized a second time by an investigation. We will minimize the disruption to your business, and safeguard your privacy and your data. Where necessary, we will seek protective orders to preserve trade secrets and business confidentiality. And we will share with you what we can, as quickly as we can, about the means and the methods of attack.

Remember that for every investigation in the news, there are hundreds that will never make the headlines. Disclosure is the exception, and not the rule. That said, we cannot act if we are not aware of the problem. Maintaining a code of silence will not benefit you or your clients in the long run.

It calls to mind the old joke about two hikers in the forest who run into a bear. The first hiker says to the other, "We just need to outrun him." And the second replies, "I don't need to outrun him. I just need to outrun you."

You may well outrun one attack, but you aren't likely to avoid the second, or the third. Our safety lies in protecting not just our own interests, but our critical infrastructure as a whole.

Conclusion

Following World War I, France built a line of concrete fortifications and machine gun nests along its borders. It was designed to give the French army time to mobilize in the event of an attack by Germany. The secondary motivation was to entice Germany to attack Belgium as the easier target.

As we all know, the Maginot Line held strong for a brief time. However, in the long run, it failed. The Germans invaded Belgium, outflanked the line, and stormed France. In the end, neither fortresses nor fortifications stopped Nazi Germany.

Our success in defeating Germany was built on a united front. We stopped playing defense, and we pushed back, day by day. No one country, standing alone, could have ended that war.

The same is true today, in this new context. No one country, no one company, and no one agency can stop cyber crime. A "bar the windows and bolt the doors" mentality will not ensure our collective safety. Fortresses will not hold forever;

walls will one day fall down. We must start at the source; we must find those responsible.
The only way to do that is by standing together. For ultimately, we all face the same threat. Together, we can and we will find better ways to safeguard our systems, minimize these attacks, and stop those who would do us harm.
Thank you all for attending this conference, and God bless.

And finally, a few comments regarding Economic Espionage:

Economic Espionage

http://www.fbi.gov/about-us/investigate/counterintelligence/economic-espionage

Introduction

The Cold War is not over, it has merely moved into a new arena: the global marketplace. The FBI estimates that every year billions of U.S. dollars are lost to foreign and domestic competitors who deliberately target economic intelligence in flourishing U.S. industries and technologies, and who cull intelligence out of shelved technologies by exploiting open source information and company trade secrets. Foreign competitors who criminally seek economic intelligence generally operate in three ways:

1. They aggressively target and recruit insiders (often from the same national background) working for U.S. companies and research institutions;

2. They conduct economic intelligence through operations like bribery, cyber intrusions, theft, dumpster diving (in search of discarded intellectual property or prototypes), and wiretapping; and,

3. They establish seemingly innocent business relationships between foreign companies and U.S. industries to gather economic intelligence, including trade secrets.

In an effort to safeguard our nation's economic secrets, the Economic Espionage Act (EEA) was signed into law on October 11, 1996.

How to Protect Your Business from Espionage: Six Steps

1. Recognize there is an insider and outsider threat to your company.
2. Identify and valuate trade secrets.
3. Implement a proactive plan for safeguarding trade secrets.

4. Secure physical and electronic versions of your trade secrets.
5. Confine intellectual knowledge on a "need-to-know" basis.
6. Provide training to employees about your company's intellectual property plan and security.

Definitions

Economic Espionage is (1) whoever knowingly performs targeting or acquisition of trade secrets to (2) knowingly benefit any foreign government, foreign instrumentality, or foreign agent. (Title18 U.S.C., Section 1831).

Trade secrets are all forms and types of financial, business, scientific, technical, economic or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically or in writing, which the owner has taken reasonable measures to protect; and has an independent economic value. "Trade secrets" are commonly called classified proprietary information, economic policy information, trade information, proprietary technology, or critical technology.

Theft of trade secrets occurs when someone (1) knowingly performs targeting or acquisition of trade secrets or intends to convert a trade secret to (2) knowingly benefit anyone other than the owner. Commonly referred to as Industrial Espionage. (Title 18 U.S.C., SECTION 1832).

A Foreign Agent is any officer, employee, proxy, servant, delegate, or representative of a foreign government.

A Foreign Instrumentality is defined as: (1) any agency, bureau, ministry, component, institution, or association; (2) any legal commercial or business organization, corporation, firm, or entity; and, (3) substantially owned, controlled, sponsored, commanded, managed or dominated by a foreign government.

Statutory authority: The Economic Espionage Act (EEA) of 1996
TERRITORIAL LIMITS: EEA protects against theft that occurs either (1) in the United States, or (2) outside the United States and (3) an act in furtherance of the offense was committed in the United States, or (4) the violator is a US person or organization.

Frequently Asked Questions

What are some methods of targeting or acquiring trade secrets?

1. Steal, conceal, or carry away by fraud, artifice, or deception;
2. Copy, duplicate, sketch, draw, photograph, download, upload, alter, destroy, photocopy, replicate, transmit, deliver, send, mail, communicate, or convey; and,

3. Receive, buy, or possess a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization.

Does the Economic Espionage Act of 1996 apply if the offender is a foreign person?

Yes. The Act states that (1) whoever knowingly performs targeting or acquisition of trade secrets to (2) knowingly benefit anyone other than the owner. Other elements will apply for prosecution.

Does the Economic Espionage Act of 1996 apply if it occurs outside the United States?

Yes. However, the violator must be (1) a US person or organization; or (2) an act in furtherance of the offense was committed in the United States.

Are there other statutes that can apply if trade secrets are not classified and therefore cannot be prosecuted under the Economic Espionage Act of 1996 Title 18 U.S.C. Section 1831 and 1832?

Yes. The following is a list of violations that may apply: mail fraud, wire fraud, interstate transportation of stolen property, export control, and misuse of a computer system. Contact your local FBI for further assistance.

Is the FBI proactive in its approach to economic espionage?

Yes. FBI Director Robert Mueller has designated counterintelligence as the FBI's number two priority, second only to counterterrorism. The Economic Espionage Unit is dedicated to countering the economic espionage threat to include developing training and outreach materials; participating in conferences; visiting private industry; working with the law enforcement and intelligence community on requirement issues; and providing specific classified and unclassified presentations.

How to Contact Us

To report violations, please contact your local field office or your nearest U.S. Embassy or consulate overseas.

ARRESTS, TRIALS AND CONVICTIONS

Chinese man sentenced in US military export case

http://www.reuters.com/article/2011/01/27/china-chitron-sentencing-idUSN2620589820110127

Thu, Jan 27 2011BOSTON | Wed Jan 26, 2011 8:26pm EST

BOSTON Jan 26 (Reuters) - A Chinese national was sentenced on Wednesday to 97 months in prison after being convicted last year of illegally exporting U.S. military equipment to China for several years, the U.S. Department of Justice said.

Department officials in Boston said that Zhen Zhou Wu, 46, traveled to the United States on an annual basis using business visas, and exported to China an array of goods. These included military electronics components and sensitive electronics used in military phased array radar, electronic warfare, and missile systems, they said.

Several Chinese military factories and military research institutes were among those to whom the defendant exported the equipment, they said.
The sentencing is the second within a week in a security case involving China, just days after Chinese President Hu Jintao wrapped up his high-profile U.S. visit.
Wu made illegal exports to China 14 times between 2004 and 2007, and filed false shipping documents with the U.S. Department of Commerce from 2005 through 2007.

"The key issue here is deterrence -- there is a real need to deter this type of conduct going forward," U.S. District Court Judge Patti Saris said during the sentencing hearing.

Wu owned and controlled a company, Chitron Electronics Inc of Waltham, Massachusetts, and used the company to procure the restricted equipment from U.S. suppliers and then export the goods to China through Hong Kong.
The exported equipment is used in electronic warfare, military radar, fire control, military guidance and control equipment, missile systems, and satellite communications.

"This defendant and corporation violated U.S. export laws and compromised our national security for more than a decade," said U.S. Attorney Carmen Ortiz.

On Friday, a Michigan man was sentenced to four years in prison for trying to get a job with the CIA so he could spy for China.

(Reporting by Ros Krasny, editing by Philip Barbara)

Former Dow Research Scientist Convicted of Stealing Trade Secrets and Perjury

http://www.justice.gov/opa/pr/2011/February/11-crm-156.html

WASHINGTON – A federal jury in Baton Rouge, La., today convicted a former research scientist of stealing trade secrets from Dow Chemical Company and selling them to companies in the People's Republic of China, as well as committing perjury, announced Assistant Attorney General Lanny A. Breuer of the Criminal Division and U.S. Attorney Donald J. Cazayoux Jr. for the Middle District of Louisiana.

After a three-week trial, the jury found Wen Chyu Liu, aka David W. Liou, 74, of Houston, guilty of one count of conspiracy to commit trade secret theft and one count of perjury.

According to the evidence presented in court, Liou came to the United States from China for graduate work. He began working for Dow in 1965 and retired in 1992. Dow is a leading producer of the elastomeric polymer, chlorinated polyethylene (CPE). Dow's Tyrin CPE is used in a number of applications worldwide, such as automotive and industrial hoses, electrical cable jackets and vinyl siding.

While employed at Dow, Liou worked as a research scientist at the company's Plaquemine, La., facility on various aspects of the development and manufacture of Dow elastomers, including Tyrin CPE. Liou had access to trade secrets and confidential and proprietary information pertaining to Dow's Tyrin CPE process and product technology. The evidence at trial established that Liou conspired with at least four current and former employees of Dow's facilities in Plaquemine and Stade, Germany, who had worked in Tyrin CPE production, to misappropriate those trade secrets in an effort to develop and market CPE process design packages to various Chinese companies.

Liou traveled extensively throughout China to market the stolen information, and evidence introduced at trial showed that he paid current and former Dow

employees for Dow's CPE-related material and information. In one instance, Liou bribed a then-employee at the Plaquemine facility with $50,000 in cash to provide Dow's process manual and other CPE-related information.
"Today a federal jury found Mr. Liou guilty of stealing protected trade secrets from Dow Chemical Company, including by bribing fellow employees for this valuable information," said Assistant Attorney General Breuer. "American industries thrive on innovation and they invest substantial resources in developing new products and technology. We will not allow individuals to steal the technology and products that U.S. companies have invested years of time and considerable money to create."

"This office will continue to pursue sophisticated and complex schemes, such as the one perpetrated by this defendant," said U.S. Attorney Cazayoux. "Such actions undermine the economic viability of our community and our nation, and will not be tolerated."

"Companies within the United States lose millions of dollars to the theft of trade secrets such as this," said Special Agent-in-Charge David Welker of the FBI's New Orleans Division. "The FBI is committed to aggressively identifying and investigating such schemes and along with our partners to bring the perpetrators to justice."

In addition, according to evidence presented at trial related to the perjury charge, Liou falsely denied during a deposition that he made arrangements for a co-conspirator to travel to China to meet with representatives of a Chinese company interested in designing and building a new CPE plant. Liou was under oath at the time of the deposition, which was part of a federal civil suit brought by Dow against Liou.

Liou faces a maximum of 10 years in prison on the conspiracy to commit trade secrets theft charge, and a maximum of five years in prison on the perjury charge. Each count also carries a maximum fine of $250,000. A sentencing date has not yet been scheduled.

The case is being prosecuted by Assistant U.S. Attorney Corey R. Amundson, who serves as the Senior Deputy Criminal Chief, and Assistant U.S. Attorney Ian F. Hipwell for the Middle District of Louisiana, as well as Trial Attorney Kendra Ervin of the Criminal Division's Computer Crime and Intellectual Property Section. The case was investigated by the FBI's New Orleans Division.

Hillsborough sheriff: McDonald's run tripped up military laptop thieves

http://www.tampabay.com/news/publicsafety/crime/article1151938.ece?bcsi-ac-75F76A8A9C5D0B36=1C6BC64F000005035ZWcm5/fGs+OVX0EsaL39ahOyjGfAAAAAwUAAKUv0AEQDgAAbwAAAGDTAQA=

By Jessica Vander Velde, Times Staff Writer

Posted: Feb 16, 2011 10:00 AM

TAMPA — They came with rappel lines, a power saw and wire cutters.
Had they only packed a lunch, the thieves who lifted $7.4 million in military laptops from an east Hillsborough warehouse last March might have savored success.

But there sat Rolando Coca, staring into a video camera at a McDonald's drive-thru, midway through the biggest cargo heist in Hillsborough history.
"That's really one of the things that broke the case for us," Hillsborough Sheriff David Gee said Wednesday.

For nearly a year, the Hillsborough County Sheriff's Office kept quiet about its investigation into the intriguing theft at iGov Technologies, which contracts with Special Operations Command. When news accidentally leaked out through a search warrant filed in July, military officials assured the public that the laptops contained no sensitive information.

Then at a news conference Wednesday morning, Sheriff David Gee announced the arrest of Coca, the 55-year-old suspected ringleader in a South Florida-based crew of about 10 thieves.

"This was very choreographed and conducted at a very high skill level," the sheriff said. "They've obviously done this before."

On the afternoon of March 6, a Saturday, two men arrived at the Palm River warehouse, climbed a maintenance ladder and cut a hole in the roof, gaining access to iGov Technologies, Gee said.

They rappelled about 20 feet down into the warehouse and cut the security systems. Then they removed the surveillance cameras outside.
But the men missed two cameras — one in the front and one in the back — a misstep that gave deputies a glimpse into the nearly 10-hour operation.

After sunset, about 10 people arrived at the warehouse and started loading the laptops into two semitrailer trucks. At about 1 a.m., they took off, and the trucks headed for Miami, a popular hub for stolen cargo.

The iGov facility manager reported the computers stolen the following Monday, and detectives started reviewing the surveillance videos. They also pulled surveillance videos from nearby businesses, looking for the red Lincoln Navigator seen coming and going from the warehouse that day.
"It was good intuition on the part of the investigators," Gee said.

Detectives hit the jackpot with a video from a nearby McDonald's drive-thru. The vehicle was recorded going through just after 10 p.m., Coca's face clearly visible. When Hillsborough detectives showed the photo to FBI investigators who specialize in cargo theft investigations, they immediately identified Coca. The FBI had already been investigating him in connection with other thefts.

Coca was indicted in December and arrested in South Florida on Jan. 25. He will be transported to Hillsborough County and tried in federal court.

The FBI made another arrest in the case, apprehending Emil Benitez in a sting. Shortly after the theft, undercover FBI officials set up a deal to pay $50,00 for some of the laptops. Benetiz was the man who accepted the money, deputies say.

In August he was sentenced to two years in federal prison.

Laptops worth about $4.7 million were found in a Miami warehouse, and authorities have been recovering other computers in smaller quantities.

They expect to make more arrests as the investigation continues.

Times news researcher John Martin contributed to this report. Jessica Vander Velde can be reached at (813) 226-3433 or jvandervelde@sptimes.com.

Iranian National Charged with Illegally Exporting Specialized Metals from the United States to Iran

http://www.justice.gov/opa/pr/2011/February/11-nsd-136.html

Some Metals Allegedly Destined for Iranian Entities Involved Ballistic Missile Activity

WASHINGTON – Milad Jafari, 36, a citizen and resident of Iran has been indicted for illegally exporting and attempting to export specialized metals from the United States through companies in Turkey to several entities in Iran, including some entities that have been sanctioned for involvement in ballistic missile activities.

The 11-count indictment, returned by a grand jury in the District of Columbia on July 21, 2010 and unsealed today, was announced by David Kris, Assistant Attorney General for National Security; Ronald C. Machen Jr., U.S. Attorney for the District of Columbia; Eric L. Hirschhorn, Under Secretary of Commerce for Industry and Security; and Sean Joyce, Executive Assistant Director of the FBI's National Security Branch.

The indictment charges Jafari with one count of conspiracy to illegally export materials to Iran and to defraud the United States; five separate counts of illegal export and attempted illegal export of materials to Iran and five additional counts of smuggling materials. The indictment also seeks forfeiture of $177,867.92 in connection with these offenses. Jafari remains at large and is believed to be in Iran. He faces a maximum potential sentence of five years in prison for the conspiracy count, 20 years in prison for each count of illegal exports to Iran, and 10 years in prison for each smuggling count.

Today, the U.S. Department of the Treasury also announced the designation of Jafari, several of his family members and associates, and several corporate entities in Iran and Turkey, under Executive Order 13382, which targets for sanctions proliferators of weapons of mass destruction and their supporters - thereby isolating them from the U.S. financial and commercial systems. According to the Treasury Department, Jafari and his associates operate a procurement network that provides direct support to Iran's missile program by securing metal products, including steel and aluminum alloys, for subordinates of Iran’s Aerospace Industries Organization (AIO).

The federal indictment unsealed today alleges that Jafari and others operated Macpar Makina San. Ve Ticaret A.S. (Macpar), a Turkish and Iranian business with locations in Istanbul and Tehran. Jafari and others also operated Standart Teknik Parca San. Ve Ticaret A.S. (STEP), a Turkish business with locations in Istanbul and Tehran.

From about February 2004 through about August 2007, the indictment alleges, Jafari engaged in a conspiracy to defraud the United States and to cause the export of goods to Iran in violation of the U.S. embargo and without the required U.S. government licenses for such exports. In carrying out the conspiracy, Jafari and his conspirators allegedly solicited orders from customers in Iran and purchased goods from U.S. companies on behalf of these Iranian customers. Jafari and others allegedly wired money to the U.S. companies as payment, concealed from the U.S. companies the end-use and end-users of the goods, and caused the goods to be shipped to Turkey and later to Iran.

Attempted Export to Sanam Industrial Group

For instance, the indictment alleges that in July 2006, Sanam Industrial Group – an entity in Iran that is controlled by Iran's AIO and has been sanctioned by the United States and United Nations for involvement in nuclear and ballistic missile activities -- issued to Jafari's company, STEP, a request for quote for 660 pounds of a specialized steel welding wire with aerospace applications. In May 2007, Jafari allegedly caused an order to be placed for 660 pounds of this exact type of welding wire with a Nevada company. The following month, the Nevada firm received more than $38,000 from Jafari's company, Macpar.

According to the indictment, Jafari made arrangements with a freight forwarder for the welding wire to be picked up from the Nevada company. The shipment was detained by the Department of Commerce's Office of Export Enforcement before it left the country. In response to questions from the Nevada company about the end-use of the welding wire, Jafari told the company that the materials "will not be exported from Turkey and will not be used for any nuclear, missile or chemical/biological weapons related applications," the indictment alleges.

In another instance, the indictment alleges that in August 2006, Heavy Metals Industries in Iran placed an order with Jafari's company, STEP, for 3,410 pounds of precipitation hardening steel made in the United States. The following year, Jafari caused Macpar to place an order with an Ohio company for 4,410 pounds of a high-grade, temperature resistant, stainless steel known to have aerospace applications. Jafari informed the Ohio firm that the steel would not be shipped to Iran. In August 2007, the stainless steel shipment was detained by the Department of Commerce's Office of Export Enforcement before it left the country.

Other Alleged Shipments to Iran

The indictment alleges that Jafari and his conspirators were successful in causing several shipments of other materials to be exported from the United States to Iran via Turkey. In July 2006, Jafari allegedly caused three kilograms of custom-made brazing alloy to be shipped from a California company to Turkey, and, in 2007, to be shipped to Iran. According to the indictment, the brazing alloy had been requested by SAPICO, also known as the Sahand Aluminum Parts Industrial Company, in Iran. SAPICO was later sanctioned in June 2010 by the United Nations for being a cover for the Shahid Hemmat Industrial Group, which is involved in Iran's ballistic missile program.

In March 2007, Jafari allegedly caused a shipment of 1,366 pounds of commercial bronze bars he purchased in the United States to be trucked from Turkey to Iran, and in September 2006, he caused electronic testing equipment to be shipped from an Illinois company to Iran via Turkey. The indictment notes

additional exports of U.S. fiber-optic equipment and aerosol generators allegedly arranged by Jafari in 2004 and 2005.

"The allegations in the indictment unsealed today shed light on the reach of Iran's illegal procurement networks and the importance of keeping U.S. materials from being exploited for Iran's weapons development," said David Kris, Assistant Attorney General for National Security. "I applaud the many agents, analysts and prosecutors who helped bring about these charges."

"The indictment unsealed today against Milad Jafari demonstrates that the United States will relentlessly pursue those who are seeking to illegally acquire U.S. goods and technology for use in Iran, and we will continue to use every tool at our disposal to protect the national security of the United States," said U.S. Attorney Ronald C. Machen, Jr. "I am proud of the efforts of our agents and prosecutors who have worked to bring this case."

"Combating illegal exports to Iran is a top priority. We are committed to choking off rogue procurement networks by every means available to us," said Under Secretary of Commerce Eric L. Hirschhorn.

"Shutting down the illegal acquisition of material destined for use in weapons programs is among the highest priorities in the FBI," said Sean Joyce, Executive Assistant Director of the FBI's National Security Branch. "We'll continue to pursue illegal acquisition efforts and protect our nation from the grave threat these WMD-related activities pose to our national security."

The investigation is being conducted by special agents of the San Jose, Calif., Washington field office and Operations Division of the Commerce Department's Office of Export Enforcement and special agents of the FBI's Charlotte, N.C., Field Division. The case is being prosecuted by Ryan Fayhee, Trial Attorney from the Counterespionage Section of the Justice Department's National Security Division, and George Varghese, Assistant U.S. Attorney from the U.S. Attorney's Office for the District of Columbia.

The details contained in the indictment are mere allegations. Defendants are presumed innocent unless and until proven guilty in a court of law.

Ford Trade Secrets Thief Pleads Guilty

http://news.softpedia.com/news/Ford-Trade-Secrets-Thief-Pleads-Guilty-167327.shtml

November 18th, 2010, 13:18 GMT

By Lucian Constantin
A Chinese national admitted to stealing trade secrets from Ford, when he left the automaker's employment and moved back to his home country in 2006. Xiang Dong Yu, aka Mike Yu, 49, of Beijing, China, worked as a product engineer for Ford Motor Company between 1997 and 2007.

At the end of 2006, Yu agreed to work for another U.S. company at its branch in China. He traveled to Shenzen on December 20, without letting Ford of his intention to quit.

According to prosecutors, upon his departure, the product engineer copied 40 confidential documents from Ford's computer to an external hard disk drive, which he took with him.

The files contained design specifications for various automotive components including engine/transmission mounting subsystem, electrical distribution system, electric power supply, electrical subsystem and generic body module.
The stolen information was the result of multi-million dollar research, development and testing efforts that spanned decades. Ford's losses were estimated at between 50 and 100 million dollars.

In January 2007 Yu officially quit his job at Ford via email and in November 2008 he went on to work for one of its direct competitors, the Beijing Automotive Company.

Yu was indicted in the Eastern District of Michigan, after the U.S. automaker discovered the data theft and contacted the FBI.

On October 19, 2009, the former product engineer traveled back to the United States for business reasons and was arrested when he landed in Chicago. Upon inspecting his company-issued laptop, investigators discovered 41 of the design specification documents stolen back in 2006. They also found evidence that all of them had been accessed in the previous months.

Yu pleaded guilty to two counts of trade secrets theft and is scheduled for sentencing on February 23 next year. He faces between 63 and 78 months in prison and a maximum fine of $150,000.

Woman sentenced for U.S. military sales to China

http://www.reuters.com/article/2011/01/28/china-chitron-sentencing-idUSN2823732820110128

BOSTON | Fri Jan 28, 2011 6:07pm EST

BOSTON Jan 28 (Reuters) - A woman who managed a Massachusetts electronics company was sentenced on Friday to three years in prison for conspiring over 10 years to export U.S. military equipment to China, U.S. authorities said.

Yufeng Wei, 46, of Belmont, Massachusetts, was convicted in 2010 of illegally exporting various goods to China, including parts on the U.S. munitions list and export-restricted technology and electronics, and for filing false shipping documents with the U.S. Department of Commerce.

The illegally exported parts were "precisely the [types of] items ... that the People's Liberation Army actively seeks to acquire," according to the U.S. Department of Defense.

The Waltham, Massachusetts company Wei managed, Chitron Electronics Inc, known as Chitron-US, was fined $15.5 million.

On Wednesday, Chinese national Zhen Zhou Wu, Chitron's owner and Wei's ex-husband, was sentenced to 97 months in prison for his role in the export conspiracy.

The defendants' enterprise involved the use of Chitron-US as a front company for its parent, Chitron Electronics Co Ltd, headquartered in Shenzhen, China, the U.S. Department of Justice said.

Wei procured export-restricted equipment from U.S. suppliers and exported them to China through Hong Kong. The equipment is used in electronic warfare, military radar, fire control, military guidance and control equipment, missile systems, and satellite communications, the DOJ said.

Chitron marketed electronics to Chinese military factories and military research institutes.

The sentences for Wei and Wu follow two other security cases involving China, just days after the high-profile visit to the United States of Chinese President Hu Jintao.
On Jan. 21, Glenn Shriver of Michigan was sentenced to four years in prison for trying to get a job with the CIA so he could spy for China.

Separately, on Jan. 25, a former Northrop Grumman Corp engineer was sentenced to 32 years in prison for providing secret defense information to China, among other crimes.

(Reporting by Ros Krasny, Editing by Eric Walsh)

TECHNIQUES, METHODS, TARGETS

COUNTER MEASURES

http://www.ft.com/cms/s/ba6c82c0-2e44-11e0-8733-00144feabdc0,dwp_uuid=03d100e8-2fff-11da-ba9f-00000e2511c8,print=yes.html

Companies should protect themselves with a mix of technical measures and common sense against disgruntled employees passing information to rivals, according to most security experts, write Joseph Menn, Peggy Hollinger, Peter Marsh and Daniel Schäfer.

While hard to measure precisely, the scale of the problem is not in doubt. The vast majority of cyber-espionage cases in the US, which are linked to "hacking" into computer networks, have been traced to e-mails with plausible-looking attachments that use parts of Microsoft Word and other commonplace programs to extract information and channel it to unauthorized people over the internet. Warnings about such espionage are often ignored by staff, however, so experts recommend that businesses focus instead on rapid patching of such software "vulnerabilities".

For added protection against potentially highly damaging leaks, every company should put in place an "anti-espionage" plan setting out who has access to sensitive data, advises Frank Hülsberg, head of compliance at the German arm of the KPMG consultancy. He also recommends that computers containing sensitive data are separated from the internet.

Often human frailty is at fault. Peter Pender-Cudlip, chief executive of London-based corporate security company GPW, says: "Behind every case of industrial

espionage sits an individual driven by the age-old motives of money, ideology, compromise or ego." It therefore follows that keeping staff reasonably happy – reducing motivation to settle scores by leaking information – is a good first principle.

On occasion, corporate theft can be linked to particular personal relationships. In a recent instance, one German engineering company found it was frequently beaten on price by a competitor. The group discovered an employee in its information technology department was related to its archrival's CEO. The IT specialist had wiretapped his own CEO's office and phone and put a tracking device on his car, enabling him to follow his movements and identify the customers to whom he was talking.

While it might seem unfair to those working in IT, security experts warn that staff in the sector are often the main sources of leaks simply because they are in a better position than others to gain access to secrets.

Industrial espionage: Data out of the door

By Jamil Anderlini in Beijing, Peter Marsh and John Reed in London, Joseph Menn in San Francisco, Peggy Hollinger in Paris and Daniel Schäfer in Frankfurt.

http://www.ft.com/cms/s/ba6c82c0-2e44-11e0-8733-00144feabdc0,dwp_uuid=03d100e8-2fff-11da-ba9f-00000e2511c8,print=yes.html

Published: February 1 2011 23:17

Last updated: February 1 2011 23:17

Jin Hanjuan was about to board a flight to Beijing almost four years ago when a random check stopped her in her tracks.

According to court documents and an FBI affidavit filed in an economic espionage case against her, when customs officers at O'Hare airport in Chicago inspected the bags of the 40-year-old software engineer, they found more than 1,000 confidential papers that are alleged to have been stolen from Motorola, the US electronics group for which Ms Jin had worked until two days before the flight.

The court papers say the officers also discovered Chinese military manuals, a European company's catalogue of military products, documents detailing Chinese

military applications for electronics equipment that had been drafted by an unnamed Chinese telecommunications company, and $30,000 in cash.

In the criminal indictment against Ms Jin, due to be heard next month in a Chicago court, Motorola says the research and development costs of the information in her possession exceed $600m. The company would lose substantial global revenues if the contents were made public, it adds. Ms Jin has pleaded not guilty.

In a separate civil case brought by Motorola, Ms Jin is a co-defendant with Huawei, the Chinese telecommunications equipment maker, over an allegation that she and others were "secretly engaged" in product development for the Chinese company at the same time as they were employed by Motorola. Huawei has said the case brought by Motorola is "without merit" and has refused to comment on the criminal case.

The legal actions involving Ms Jin have thrown the spotlight on the murky world of industrial espionage – defined as the use of illicit means by companies or their agents to disrupt their rivals' operations or gain access to their secrets.

Interest in the subject has been heightened by a highly publicized affair in France that has led to Renault, the automotive group, sacking three top executives after alleging they had passed on confidential documents to outsiders. According to Carlos Ghosn, the group's chief executive, the alleged theft relates to the company's business model for battery powered electric cars – an area where Renault and Nissan, its Japanese partner that Mr. Ghosn also heads, are investing €4bn ($5.5bn) in a significant early bet on the technology.

Industrial espionage is being catapulted to a position of great relevance to many of the world's top companies as technological change becomes of growing importance to business performance. Companies across the world are increasingly interested in gaining access to their competitors' secrets as early as possible in the development cycle for new products and services.

"There is ... more globalization and the players are more ... in competition. The more competition, the more crime," says Olivier Buquen, head of the Economic Intelligence Office in Paris, a bureau of 12 experts created in 2009 to co-ordinate French corporate intelligence efforts.

According to Dane Chamarro, managing director for North Asia at Control Risks, a security group, industrial espionage affects many more sectors than high-profile activities such as computers, cars and telecoms. "Virtually any company with high levels of research and development and where technology has an impact on the product faces some kind of threat," he says.

The chief executive of one of the world's biggest aerospace and defence groups says that in his industry, "industrial espionage is a problem now and it will be even more in the future".

Most corporate intelligence gathering is legitimate, based on such conventional practices as picking up scraps of information about competitors by attending trade shows. But few people involved doubt that the illicit part of this activity is bigger than it ever was.

The ways that secrets are taken vary. One of the most widely used is when employees switch jobs, taking with them confidential designs. Andrea Riello, chief executive of Riello, a large Italian machine tool maker, says: "In our company, we've seen three times in five years that some of our technical secrets have been taken and used in a rival's products. In each case it seems as though a former employees has taken details to other businesses." The practical difficulties in gathering evidence mean, Mr. Riello adds, that his company has not yet tried to seek legal redress for the "theft" of technologies.

Other instances can be more unusual. One French engineering supplier found that an engineer from an Asian company when visiting its factory stooped to lace up his shoes more often than seemed necessary. The ruse was intended to collect tiny pieces of metal from the floor – discarded from machining operations – that were picked up with a piece of tape on his overlong tie and could later be analysed by a rival business.

Taking into account all types of industrial espionage but counting only the cost to American businesses, US intelligence officials put the cost of lost sales due to illicit appropriation of technology and business ideas at $100bn-$250bn a year. General Motors, Ford, General Electric, Intel and Boeing are among the US companies known to have suffered from industrial espionage attacks, though all are wary of discussing the details.

In Europe, concerns about the loss of technical know-how have resulted in a push in Brussels for the European Commission to set up a group to monitor foreign investment activity.

According to many people involved with corporate intelligence, Beijing state agencies are often heavily involved in efforts by Chinese companies to gather information about foreign businesses. Russia, France and Israel also have active state-led programmes as well as corporate programmes to appropriate technology from foreign companies but China's methodical approach is regarded as unique by many in the corporate security industry.

One veteran corporate security manager working for large multinational companies in China says Washington considers that country the biggest threat in terms of targeting US companies' commercial proprietary information, technical information and data. Nigel Inkster, a director at the London-based International Institute for Strategic Studies, warned in a speech last month, meanwhile that commercial espionage was now a "big business" with countries such as China engaged in the activity "on an industrial scale".

While some of this stems from the blurry line that separates the government and companies in a country where many of the big guns of industry are state-controlled, another factor is history. Twenty-five years ago next month, Deng Xiaoping, China's leader of the time, approved a government programme that would become known as the "863 project" (named after the date – the third month of 1986). The 863 programme still exists and is funded and administered by the Beijing government.

Its stated goal is to stimulate advanced technologies in a range of fields, to render China independent of financial obligations for foreign technologies. Many in the west believe, however, that its remit in reality extends to backing the illicit acquisition of foreign proprietary technology.

Whatever the scale and scope of the 863 unit's activities, China's state-led industrial espionage operations are uniquely patient and cautious, say China-based economic intelligence experts – a way of working known as the "thousand grains of sand" approach.

They collect "whatever they can in a very broad area that they're interested in and then they patiently distil their finding down until they get what they need", according to one corporate security chief working in China. "Their approach contrasts significantly with the Russians, who tend to be overly ambitious and clumsy by comparison."

The form can vary from paying employees to hand over information or gathering know-how about processes or products while on factory visits, through to cyber-attacks based around hacking into databases or electronic networks.

Cyber-spying has fast become a specific threat for many companies. "Industrial cyber-espionage is one of the biggest problems that all nations are facing," says Melissa Hathaway, a former US intelligence official and the leader of a digital security review set up by President Barack Obama.

The scale of hacking to gain corporate information has gone so far, she says, that the Securities and Exchange Commission, the US stock market regulator,

might soon need to require companies to assess routinely for the benefit of shareholders how well they are protecting themselves from electronic attacks. One of the most high-profile companies to have suffered in this way is Google. After announcing last year that it had been the victim of a sophisticated hacking campaign from China, it emerged that attackers had appropriated some of Google's search engine source codes, a vital piece of intellectual property. Google later notified more than a dozen other companies it identified as victims of the same campaign. Outside researchers later concluded that more than 100 concerns had been hit, including a big investment bank, other high-technology hardware and software companies and defence contractors. Among those in the Chinese sights were Symantec, Adobe Systems and Northrop Grumman. In all cases, the target was intellectual property, including software codes, chip designs and the like.

The campaign originated on computers used at two universities in China, one of which has strong ties to the military. While the Chinese government publicly denies that it engages in industrial espionage or computer hacking, this view is regarded by many foreign companies as intelligence agencies as being some way from the truth.

What should companies do about the threat of industrial espionage? One answer may be to minimize the possibility of leakages either through elaborate information technology methods or sometimes ideas that owe more to plain common sense. Another may be to abandon any hope that all leaks can be plugged and concentrate on the most advanced technologies and products that are all but impossible to replicate by any outsider due to their complexity and the use of novel ideas.

Dieter Zetsche, chief executive of Daimler, the German automotive group, says he has "no concerns" about a theft of his company's secrets. "We shouldn't waste our time trying to protect our intellectual property but try to be innovative and faster than the other guys."

That said, efforts to crack down on thefts of technology or other valuable business information seem likely to be central to companies' efforts to stay competitive – especially in sectors such as machine building or high-tech engineering products, where the developed world retains a commercial edge. Back in the US, when Ms Jin arrives at the Chicago court in the coming weeks, she faces six counts of trade theft and economic espionage, each carrying a potential penalty of 10-15 years in prison and a fine of as much as $500,000. If she is found guilty, a lot of people interested in thwarting industrial espionage in all its forms will raise a small cheer.

Additional reporting by Peggy Hollin-ger, Joseph Menn, John Reed, Daniel Schäfer and Nikki Tait

Exxon, Shell, BP Said to Have Been Hacked Through Chinese Internet Servers

http://www.bloomberg.com/news/print/2011-02-24/exxon-shell-bp-said-to-have-been-hacked-through-chinese-internet-servers.html

By Michael Riley - Feb 24, 2011 Computer hackers working through Internet servers in China broke into and stole proprietary information from the networks of six U.S. and European energy companies, including Exxon Mobil Corp., Royal Dutch Shell Plc and BP Plc, according to one of the companies and investigators who declined to be identified.

McAfee Inc., a cyber-security firm, reported Feb. 10 that such attacks had resulted in the loss of "project-financing information with regard to oil and gas field bids and operations." In its report, Santa Clara, California-based McAfee, assisted by other cyber-security firms, didn't identify the energy companies targeted. The attacks, which it dubbed "Night Dragon," originated "primarily in China" and occurred during the past three years.

The list of companies hit, none of which disclosed the attacks in filings with regulators, also includes Marathon Oil Corp., ConocoPhillips and Baker Hughes Inc., according to the people who worked on or are familiar with the companies' investigations and asked not to be identified because of the confidential nature of the matter.

Chinese hackers broke into the computer network of Baker Hughes, said Gary Flaharty, spokesman for the Houston-based provider of advanced drilling technology. Baker Hughes concluded the incident didn't need to be disclosed because it wasn't material to investors, he said, declining to comment further.

Undetected Access

In some of the cases, hackers had undetected access to company networks for more than a year, said Greg Hoglund, chief executive officer of Sacramento, California-based HBGary Inc., a cyber-security company that investigated some of the security breaches at oil companies. Hoglund, who was cited by McAfee as a contributor to its report, declined to identify his clients.

"Legal information, information on deals and financial information are all things that appear to be getting targeted," Hoglund said, summing up conclusions his firm made from the types of documents and persons targeted by the hackers.

"This is straight up industrial espionage."

Hackers targeted computerized topographical maps worth "millions of dollars" that show locations of potential oil reserves, said Ed Skoudis, whose company, Washington-based InGuardians Inc., investigated two recent breaches of U.S. oil companies' networks. He declined to name his clients or the origin of the hackers.

'Unsophisticated' Techniques

The McAfee report described the techniques used to get into the energy company computers as "unsophisticated" and commonly used by Chinese hackers. The attacks began in November 2009, McAfee said. Two cyber investigators familiar with the probes said the attacks began even earlier -- in 2008 -- and involved several well-financed groups. The investigators asked not to be identified because the company investigations are private.

McAfee based the report on information gathered from its own work on the breaches and from others who were directly involved in investigating them. The report, produced on the condition that the affected companies not be identified, was done to "educate the community," said Ian Bain, a McAfee spokesman. The thefts of oil company data like those in the McAfee report match the profile of industrial espionage operations that have the backing or consent of the Chinese government, said Joel Brenner, former head of U.S. counterintelligence during the Bush and Obama administrations and now a lawyer with Cooley LLP in Washington. In his former post, one of Brenner's jobs was tracking spying efforts against U.S. companies from foreign countries.

'On the Hunt'

"The Chinese are on the hunt for natural resources to fuel this massive economic leap forward," Brenner said.

Ma Zhaoxu, spokesman for China's Ministry of Foreign Affairs, said he had no information about the attacks on the oil companies when asked about the issue at a regular briefing today.

"The Chinese government opposes hacking activities," Ma said. "China falls victim to hacking itself. We will step up efforts to crack down on hacking crimes."

The thefts might trigger legal liability for companies that chose not to disclose them to investors, said Blair Nicholas, a San Diego-based partner at law firm Bernstein Litowitz Berger and Grossman.

"To the extent that there aren't adequate procedures in place to protect the companies' crown jewels and somebody gets the key to jewelry box, there is certainly potential for shareholder derivative liability," Nicholas said.

Securities Laws

Investors might also argue they had a right under U.S. securities laws to be informed of the thefts, which a judge might construe as a "material" fact that should have been disclosed, Nicholas said.

John Roper, a spokesman for Houston-based ConocoPhillips; Lee Warren, a Marathon Oil spokeswoman at its Houston headquarters, and Alan Jeffers, a spokesman for Irving, Texas- based Exxon, said in e-mail messages that their companies don't comment on security-related issues. David Nicholas, a spokesman for London-based BP, and Kim Blomley, a spokesman in London for Shell, which is based in The Hague, declined to comment.

Jenny Shearer, an FBI spokeswoman in Washington, said she couldn't comment on whether the agency was investigating the attacks. Laura Sweeney, a Justice Department spokeswoman, said the department can't comment on a possible investigation.

Hacker Activists

Some aspects of the attacks were disclosed in internal e- mails made public after a February security breach at HBGary. The e-mails were stolen from HBGary's computer network by the group of hacker activists called Anonymous, which posted them on the Internet.

"I've been able to confirm that the same attackers are conducting coordinated IP thefts against Baker Hughes and Shell Oil, going after bid data and operational reporting, as well as projects/plans and related financial information," according to an e-mail written on Jan. 13 by an independent security consultant working on the cases.

"I reached out to some friends at Conoco and Exxon and they also experienced similar breaches," the consultant wrote in the e-mail. "This is of course client confidential," he added under the subject line "coordinated Chinese attacks on oil companies."

In a separate e-mail, an HBGary investigator discussed the analysis of malware designed to steal data in the computers of a drilling rig working on a ConocoPhillips project.

Marc Zwillinger, an attorney representing HBGary, declined to comment on the e-mails' content.

'Stolen E-Mails'

"Those are stolen e-mails and they contain confidential information relating to clients," Zwillinger said.

The McAfee report, which cites several attacks connected to the Chinese hacking underground, doesn't link the "Night Dragon" attack directly to the Chinese government.

Analysts who assessed the attacks on energy companies said the source of the breaches was easier to pinpoint than in previous hits by Chinese hackers, including an attack against Google Inc. that that company disclosed in January 2010.

The hackers used tools prevalent in China's underground hacking forums, the McAfee report said, and they appeared to work from 9 a.m. to 5 p.m., Beijing time. McAfee traced the hackers' command-and-control operations to servers operated by a company in China's Heze City in Shandong province.

The owner of the company, Song Zhiyue, said he wasn't aware of any hacking taking place from his servers and that he always seeks to verify the activities of customers who rent server space from him.

"There are so many servers in the world," Song said. "This has nothing to do with me. This is very unfair."

Woman arrested in impersonation of FBI agent

BY VIK JOLLY

http://www.ocregister.com/news/fbi-287881-hanover-caller.html

THE ORANGE COUNTY REGISTER

The Seal Beach woman allegedly used "spoofing" technology in the impersonations, according to the intelligence agency

Updated: Feb. 11, 2011 10:39 a.m.

SANTA ANA – Federal agents arrested a Seal Beach woman Thursday on suspicion of using "spoofing" technology to impersonate FBI agents in telephone calls to business clients who believed she was running a fraud scheme, according to an FBI news release.

Karen Elaine Hanover, 44, was arrested without incident at Fashion Island in Newport Beach by FBI special agents. Hanover was charged with impersonating a federal agent in a criminal complaint filed Tuesday in U.S. District Court in Santa Ana.

If convicted, she faces a maximum penalty of three years in federal prison and a fine of up to $250,000.

A separate investigation into the fraud allegations is under way, FBI spokeswoman Laura Eimiller said.

Congress acted late last year to address "spoofing," where scammers use the caller ID of, for example, a bank or a government office to deceive people into giving them private information.

The law enacted in December exempts law enforcement or intelligence activities and certain other organizations but applies to those who use caller ID, the number appearing on the phone of the person receiving the call, to defraud, cause harm or wrongfully obtain anything of value. It authorizes civil penalties of as much as $10,000 for each violation, as much as $1 million for any single act. The "spoofing" technology that allows people to not only use someone else's caller ID but also disguise their voice doesn't appear to be illegal. "My understanding is that the technology itself is not illegal," Eimiller said.

During the second half of 2010, one of Hanover's unsatisfied clients was contacted by telephone by a caller with a male voice who claimed to be an FBI agent and whose caller ID was for the main number of the FBI's Los Angeles field division, the news release said.

In this call, the "agent" threatened to have Hanover's client, a Buena Park woman, imprisoned if she did not stop harassing Hanover, according to the affidavit in support of the complaint.

Subsequent investigation revealed that calls from the purported male FBI agent were actually made from Hanover's cellular phone, who allegedly used a website to alter her voice and to alter her caller ID to "spoof" the FBI's phone number, the FBI said.

Further investigation revealed that Hanover had used this website to "spoof" the FBI Miami division's phone number, as well as the intelligence agency's headquarters number in Washington, D.C., in an effort to discourage disgruntled clients from complaining to the authorities, the release says.

According to the affidavit, Hanover operated a real estate service that charged investors a $30,000 fee in exchange for providing information about finding and acquiring commercial properties, offering most clients a money-back guarantee.

The FBI started receiving complaints in July 2010 about a real estate fraud scheme.

When some clients concluded that Hanover failed to deliver the promised services, the FBI said, they complained about Hanover's operation on a blog and encouraged others to report Hanover's fraudulent activity to the FBI and other federal authorities.

The Associated Press contributed to this report.

Contact the writer: 714-834-3773 or vjolly@ocregister.com

Worldwide Caution

This information is current as of today, Tue Feb 01 12:45:28 2011.
January 31, 2011

The Department of State has issued this Worldwide Caution to update information on the continuing threat of terrorist actions and violence against U.S. citizens and interests throughout the world. U.S. citizens are reminded to maintain a high level of vigilance and to take appropriate steps to increase their security awareness. This replaces the Worldwide Caution dated August 12, 2010, to provide updated information on security threats and terrorist activities worldwide.

The Department of State remains concerned about the continued threat of terrorist attacks, demonstrations, and other violent actions against U.S. citizens and interests overseas. U.S. citizens are reminded that demonstrations and

rioting can occur with little or no warning. Current information suggests that Al-Qaida and affiliated organizations continue to plan terrorist attacks against U.S. interests in multiple regions, including Europe, Asia, Africa, and the Middle East. These attacks may employ a wide variety of tactics including suicide operations, assassinations, kidnappings, hijackings, and bombings.

Extremists may elect to use conventional or non-conventional weapons, and target both official and private interests. Examples of such targets include high-profile sporting events, residential areas, business offices, hotels, clubs, restaurants, places of worship, schools, public areas, and locales where U.S. citizens gather in large numbers, including during holidays.

U.S. citizens are reminded of the potential for terrorists to attack public transportation systems and other tourist infrastructure. Extremists have targeted and attacked subway and rail systems, as well as aviation and maritime services. In the past several years, these types of attacks have occurred in cities such as Moscow, London, Madrid, and Glasgow.

Current information suggests that Al-Qaida and affiliated organizations continue to plan terrorist attacks against U.S. and Western interests in Europe. European governments have taken action to guard against terrorist attack and some have spoken publicly about the heightened threat conditions. In the past several years, attacks have been planned or occurred in various European cities.

Credible information indicates terrorist groups also seek to continue attacks against U.S. interests in the Middle East and North Africa. For example, Iraq remains dangerous and unpredictable. Attacks against military and civilian targets throughout Iraq continue. Methods of attack have included roadside improvised explosive devices, mortars, and shootings; kidnappings still occur as well. Security threat levels remain high in Yemen due to terrorist activities there. The U.S. Embassy has had to close several times in response to ongoing threats by Al-Qaida in the Arabian Peninsula (AQAP). U.S. citizens as well as other Westerners have been targeted for attack in Yemen. U.S. citizens have also been the targets of numerous terrorist attacks in Lebanon in the past (though none recently) and the threat of anti-Western terrorist activity continues to exist there. In Algeria, terrorist attacks occur regularly, particularly in the Kabylie region of the country. In the past, terrorists have targeted oil processing facilities in both Saudi Arabia and Yemen.

A number of Al-Qaida operatives and other extremists are believed to be operating in and around Africa. Since the July 11, 2010, terrorist bombings in Kampala, Uganda, for which the Somalia-based, U.S.-designated Foreign Terrorist Organization al-Shabaab has claimed responsibility, there have been increased threats against public areas across East Africa. The terrorist attacks of

August and September 2010 against the Transitional Federal Government (TFG) and African Union (AU) peacekeeping forces in Somalia, as well as the bombing of hotels and minibuses in Somalia, highlight the vulnerabilities to terrorist attacks in East Africa and around the world. Additionally, the terrorist group, Al-Qaida in the Islamic Maghreb (AQIM), has declared its intention to attack Western targets throughout the Sahel (which includes Mali, Mauritania, and Niger), and has claimed responsibility for kidnappings, attempted kidnappings, and the murder of several Westerners.

U.S. citizens considering travel by sea near the Horn of Africa or in the southern Red Sea should exercise extreme caution, as there has been a notable increase in armed attacks, robberies, and kidnappings for ransom by pirates. Merchant vessels continue to be hijacked in Somali territorial waters, while others have been hijacked as far as 1,000 nautical miles off the coast of Somalia, Yemen, and Kenya in international waters.

The U.S. government maritime authorities advise mariners to avoid the port of Mogadishu and to remain at least 200 nautical miles off the coast of Somalia. In addition, when transiting around the Horn of Africa or in the Red Sea, it is strongly recommended that vessels travel in convoys and maintain good communications at all times. U.S. citizens traveling on commercial passenger vessels should consult with the shipping or cruise-ship company regarding precautions that will be taken to avoid hijacking incidents. Commercial vessels should review the Department of Transportation Maritime Administration's suggested piracy countermeasures for vessels transiting the Gulf of Aden.

The U.S. government continues to receive information that terrorist groups in South and Central Asia may also be planning attacks in the region, possibly against U.S. government facilities, U.S. citizens, or U.S. interests. The presence of Al-Qaida and its affiliates, Taliban elements, Lashkar-e-Taiba, indigenous sectarian groups, and other terror organizations, many of which are on the U.S. government's list of Foreign Terror Organizations (FTOs), poses a potential danger to U.S. citizens in the region. Terrorists and their sympathizers have demonstrated their willingness and ability to attack targets where Americans or Westerners are known to congregate or visit. Their actions may include, but are not limited to, vehicle-born explosive attacks, improvised explosive device attacks, assassinations, carjackings, rocket attacks, assaults, or kidnappings. Examples of potential attacks in South Asian states include Pakistan, where a number of extremist groups continue to target U.S. and other Western citizens and interests, and Pakistani government officials and military/law enforcement personnel. Suicide bombing attacks continue to occur throughout the country on a regular basis, often targeting government authorities such as police checkpoints and military installations, as well as public areas such as mosques, and shopping areas. In Afghanistan, remnants of the former Taliban regime and

the Al-Qaida terrorist network, as well as other groups hostile to International Security Assistance Force (ISAF)/NATO military operations, remain active. There is an ongoing threat to kidnap and assassinate U.S. citizens and Non-Governmental Organization (NGO) workers throughout the country. In India, there is a continuing threat of terrorism as attacks have randomly targeted public places frequented by Westerners, including luxury and other hotels, trains, train stations, markets, cinemas, mosques, and restaurants in large urban areas.

Supporters of terrorist groups such as the Islamic Movement of Uzbekistan, Al-Qaida, the Islamic Jihad Union, and the Eastern Turkistan Islamic Movement are active in the Central Asian region. Members of these groups have expressed anti-U.S. sentiments and have attacked U.S. government interests in the past. Previous terrorist attacks conducted in Central Asia have involved improvised explosive devices, suicide bombings, assassinations, and kidnappings.

Before You Go

The Department of State encourages U.S. citizens living overseas or planning to travel abroad are encouraged to enroll in the Smart Traveler Enrollment Program (STEP). By enrolling in STEP, we can keep you up to date with important safety and security announcements. Enrolling in STEP will also make it easier for the Embassy to contact you in the event of an emergency. You should remember to keep all of your information in STEP up to date; it is particularly important when you enroll or update your information to include a current phone number and e-mail address.

U.S. citizens are strongly encouraged to maintain a high level of vigilance, be aware of local events, and take the appropriate steps to bolster their personal security. For additional information, please refer to "A Safe Trip Abroad". U.S. government facilities worldwide remain at a heightened state of alert. These facilities may temporarily close or periodically suspend public services to assess their security posture. In those instances, U.S. embassies and consulates will make every effort to provide emergency services to U.S. citizens. U.S. citizens abroad are urged to monitor the local news and maintain contact with the nearest U.S. Embassy or Consulate.

As the Department of State continues to develop information on potential security threats to U.S. citizens overseas, it shares credible threat information through its Consular Information Program documents, such as Travel Warnings and Travel Alerts as well as Country Specific Information, which are available on the Bureau of Consular Affairs website. Stay up to date by bookmarking our Bureau of Consular Affairs website. Follow us on Twitter and the Bureau of Consular Affairs page on FaceBook as well.

In addition to information on the Internet, travelers may obtain up-to-date information on security conditions by calling 1-888-407-4747 toll-free in the United States and Canada or, outside the United States and Canada, on a regular toll line at 1-202-501-4444. These numbers are available from 8:00 am to 8:00 pm Monday through Friday, Eastern Time (except U.S. federal holidays).

Sea Launch Company Emerges From Chapter 11

http://www.prnewswire.com/news-releases/sea-launch-company-emerges-from-chapter-11-106122943.html

LONG BEACH, Calif., Oct. 28 /PRNewswire/ -- Sea Launch Company has successfully completed its Chapter 11 reorganization process, effective October 27, 2010. As part of the court-approved Plan of Reorganization, Energia Overseas Limited (EOL), a Russian corporation, will have acquired a majority ownership of the reorganized Sea Launch entity.

The Plan of Reorganization was approved by Judge Brendan Shannon, in the U.S. Bankruptcy Court in Wilmington, Delaware, on July 27, 2010. The successor entity, Sea Launch S.a.r.l., will be responsible for corporate functions at its operations headquarters and will maintain some assets at Sea Launch Home Port, in the Port of Long Beach, in Southern California.

Energia Logistics Ltd., a U.S. corporation, will assume management of rocket assembly and satellite integration operations at the existing Sea Launch Home Port facilities. A Moscow- based EOL-affiliate will manage supply chain operations of all CIS-based primary and second-tier suppliers for the Sea Launch system. The reliable Zenit-3SL launch system and its experienced operations team, with a history of 30 launches to date, will continue to support future launches.

Kjell Karlsen, Sea Launch president and general manager, and Brett Carman, chief financial officer – as well as some of the senior members of Sea Launch's executive management team – are transitioning to the new Sea Launch entity and will be joined by new professionals who will be added to the Sea Launch team as it returns to full flight operations.

Leading up to the closing of the transaction with EOL, Sea Launch successfully completed a series of milestones in 2009-10, followed by U.S. Government review of the new ownership structure. The transaction cleared the Committee on Foreign Investment in the United States on September 8, 2010.

"We are thrilled to have successfully emerged from Chapter 11 with a solid financial structure and a healthy manifest of future launches," said Karlsen.

"Completing this transaction will represent a significant accomplishment in the final steps toward re-entering the market as a strong and competitive commercial launch service provider. We are now planning for our return to launch operations in 2011, building on the continuity of our collective expertise and proven experience of our launch system and our team.

"I want to thank everyone involved in supporting this effort, including our dedicated employees, partners and suppliers, as well as our advisors and customers, who have trusted us to provide future access to space for their satellites. We could not have succeeded in this endeavor without their commitment and support."

"We had an opportunity to systematically analyze all the existing processes and operations, both internal and external, and as a result, we are talking about an overhaul of the business at all levels," said Dennis Shomko a spokesman for EOL. "For customers, that means transparency, reliability and predictability. We are confident that we can deliver a competitive level of 'business comfort' to them, while ensuring that our suppliers are managed appropriately."

Sea Launch is currently gearing up its operations and conducting maintenance of all launch related systems, while at the same time preparing for a Land Launch mission slated for as early as the 1st Quarter of 2011. This mission, the launch of the Intelsat-18 communications satellite, will originate from the Baikonur Space Center in Kazakhstan. The next mission from the equatorial launch site is planned for the 3rd Quarter of 2011. The world's only ocean-based launch operations originate from the Odyssey Launch Platform, positioned at 154 degrees West Longitude, in international waters of the Pacific Ocean. Jefferies & Company, Alston & Bird and Chris Picone of Buccino & Associates, Inc., served as advisors to Sea Launch. Salans, LLP, and Avicon (UK) served as advisors to Energia Overseas Limited.

About Sea Launch Company

Sea Launch Company LLC, headquartered in Long Beach, Calif., offers the most direct and cost-effective route to geostationary orbit for heavy commercial communications satellites. Sea Launch also offers Land Launch services for medium weight satellites, with launch operations originating from the Baikonur Space Center in Kazakhstan. For more information, please visit the company website at: www.sea-launch.com

Contact:

Chris Picone, 312.629.1200 or 773.936.6626, chrisp@buccinoassociates.com
Peter Stier, 562.499.4726 or 562.254.5895, peter.g.stier@sea-launch.com

SOURCE Sea Launch Company LLC

Hacking with USB keyboard emulators

http://www.h-online.com/security/news/item/Hacking-with-USB-keyboard-emulators-1172612.html

It's common knowledge that, due to the risk of infection, caution needs to be exercised when connecting USB flash drives to a PC. What's not so well known is that modified USB devices can also pose as keyboards and immediately pass keystrokes to a victim's system.

Depending on the operating system, just a few emulated keystrokes can be enough to sabotage or infect a system – mouse emulation is also possible. In contrast to USB flash drives, when a keyboard is connected the operating system will not usually display a window requesting permission to use the device. A user may not even be aware that a modified USB device posing as a human interface device (HID) has been connected to his or her system. Under Windows a pop-up window is briefly displayed, but under Linux only a glance at the logs will reveal that this has occurred.

Until recently, hackers were using micro-controller boards with USB support, such as the Teensy USB Development Board, for such attacks. This kind of hardware has been used to hack the PS3, for example. At the recent Black Hat Conference, however, security specialists Angelos Stavrou and Zhaohui Wang presented a talk on how to hack PCs without the aid of specialist hardware. By applying a simple modification to the USB stack on an Android mobile, they were able to make it pose as a keyboard when connected to a computer.

Stavrou and Wang have not so far made their software publicly available. However, toolkits for programming and loading the Teensy board with special payloads have been around for a while. The Social Engineering Toolkit, for example, works in combination with the Metasploit exploit framework to open a shell on the target system which can be accessed via a local network.

The idea of using crafted USB devices originally arose some (German language link) years ago as a joke. A prank gadget, available as the Phantom Keystroker, is designed to drive colleagues or partners mad by emulating keystrokes and mouse movements. ThinkGeek, the company behind the Phantom, is keen to emphasize that version 2.0 of the device never actuates the left mouse button or the enter key, ensuring that it can't cause any actual damage.

Official: 100 foreign agencies test US networks

(AP)

http://www.google.com/hostednews/ap/article/ALeqM5iGMAInxaJxFPslHG0_RAnRkjuEqQ?docId=f77c72e6081742d39398fd45bd36eadc

WASHINGTON (AP) — More than 100 foreign intelligence agencies have tried to breach U.S. defense computer networks, largely to steal military plans and weapons systems designs, a top Pentagon official said Tuesday.
Deputy Defense Secretary William Lynn said that while foreign governments and rogue states may try to launch more destructive attacks against military networks, most may stick to theft and spying because they are worried about a U.S. counterattack.

The greater threat, he said, are terror groups such as al-Qaida, who are more difficult to deter. Terrorists have vowed to unleash cyberattacks, and over time may be able to either develop their own malicious computer threats or buy them on the black market.

Lynn's remarks, made at a cybersecurity conference in San Francisco and released in Washington, come as the U.S. government is struggling to ramp up its abilities to block cyberintrusions and to lay out policies for launching the high-tech attacks when needed. U.S. government sites are scanned and attacked millions of times a day, and there have been a number of serious breaches in recent years, including into the electric grid and Pentagon weapons contractors.
In a meeting with reporters after his speech, Lynn declined to specify how many of the 100 foreign intelligence agencies that he says have tried attacks on the U.S. were successful in breaching government defenses, saying that would include classified information. He said the attacks involved espionage, such as seeking weapons design or diplomatic information, and didn't appear to be aimed at causing destruction of physical infrastructure.

The biggest challenge faced by the U.S. as it looks to better gird against attacks, Lynn said, is finding ways to share threat information with private industry — which owns or operates as much as 85 percent of the networks. Those include much of the nation's critical infrastructure, ranging from the electric grid, banking and other financial systems and nuclear power plants.

The idea raises privacy concerns with the prospect of U.S. military or government eyes or ears on private networks.

Lynn said the government's intelligence capabilities give it broad knowledge of cyberthreats, and the U.S. already has shared unclassified information on a limited basis with defense companies that have sensitive data on their networks. The challenge, he said, is developing the policies and legal structure so that classified information about threats can also be shared.

Lynn also unveiled two new programs that will allow the government and industry to exchange cybersecurity experts and make better use of National Guard and Reserve members who have technological expertise.
Associated Press writer Jordan Robertson in San Francisco contributed to this report.

French warn of Chinese industrial espionage

http://www.theage.com.au/action/printArticle?id=2163972

February 3, 2011 - 3:00AM

CHINA is using honey traps and spying interns in industrial espionage, according to leaked French intelligence files.

One report claimed a top French researcher was wined and dined by a Chinese woman and ended up in bed with her.

"When he was shown the recorded film of the previous night in his hotel room … he proved highly co-operative," an intelligence official said.

In another case, an unnamed French company realized that a sample of its patented liquid had left the building after a visitor from a Chinese delegation dipped his tie into the liquid to take home a sample.

Companies should do more to protect themselves from prying eyes among the 30,000 Chinese students on internships in France, experts warned.

One of the most frequent methods cited by French intelligence involves international tenders for business. When Western companies compete, "each [company] tries to outdo the other, once, twice, several times, until the Chinese consider they've had enough". Then bidders are told the project has been shelved and the information is used by the Chinese to develop their own products.

A prime example was a recent tender to build China's high-speed train. During bidding by France's TGV, the government organised a six-month training course for Chinese engineers. Soon afterwards China brought out its own high-speed train, remarkably similar to the TGV.

Chinese cyber-spies penetrate Foreign Office computers

http://www.guardian.co.uk/world/2011/feb/04/chinese-super-spies-foreign-office-computers/print

William Hague told security conference that an attack was repelled from 'a hostile state intelligence agency'

Richard Norton-Taylor and Julian Borger in Munich guardian.co.uk, Friday 4 February 2011 21.01 GMT

China has penetrated the Foreign Office's internal communications in the most audacious example yet of the growing threat posed by state-sponsored cyber-attacks, it emerged tonight.

William Hague told a security conference in Munich that the FO repelled the attack last month from "a hostile state intelligence agency". Although the foreign secretary did not name the country behind the attacks, intelligence sources familiar with the incidents made it clear he was referring to China. The sources did not want to be identified because of the sensitive nature of the issue.
In his speech Hague was reflecting growing anger and concern within the government about the increasing threat posed by cyber-espionage – states, as well as individuals, using cyberspace to steal defence, diplomatic and commercial secrets.

"It is a new development. The UK is prepared to admit the attacks were state-backed," said Alexander Neill, head of the Asia programme at the Royal United Services Institute think-tank.

The foreign secretary said the FO attack came in the form of an email sent to three of his staff "which claimed to be about a forthcoming visit to the region and looked quite innocent". "In fact it was from a hostile state intelligence agency and contained computer code embedded in the attached document that would have attacked their machine. Luckily, our systems identified it and stopped it from ever reaching my staff," Hague said.

In another attack last year, the foreign secretary said Britain's defence industry was "deliberately" targeted. "A malicious file posing as a report on a nuclear

Trident missile was sent to a defence contractor by someone masquerading as an employee of another defence contractor," Hague told an audience of western officials and businessmen. "Security meant that the email was detected and blocked, but its purpose was undoubtedly to steal information relating to our most sensitive defence projects."

Hague admitted that a third attack, apparently criminal, had succeeded in evading Britain's defences, with a version of the Zeus malware widely used to extract banking information and other personal details from targeted computers.

"In late December a spoof email purporting to be from the White House was sent to a large number of international recipients who were directed to click on a link that then downloaded a variant of Zeus," Hague said. "The UK government was targeted in this attack and a large number of emails bypassed some of our filters. Our experts were able to clear up the infection, but more sophisticated attacks such as these are becoming more common."

The foreign secretary said government was spending £650m on its cyber defences against such attacks, and working with the private sector. But he added that the international response was "fragmented and lacks focus".

Speaking to journalists later, Hague said: "We're witnessing an exponential rise in the misuse of cyberspace. In a decade, this could be out of control, and we have to start to do the thinking now."

He said Britain was offering to host an international conference this year aimed at establishing global standards.

"Many countries do not share our view of the positive impact of the internet, and others are actively working against us in a hostile manner," he said.

"However as liberal democracies we also have a compelling interest in supporting democratic ideals in cyberspace, and working to convince others of this vision."

General Sir David Richards, chief of the defence staff, last month said the UK needed its own Cyber Command, similar to that set by the US defence department. He said that the advance of cyber technology would lead to a "cultural change" in warfare which the UK must be prepared for."We must learn to defend, delay, attack and maneuver in cyberspace, just as we might on the land, sea or air and all together at the same time".

CYBER, HACKING, DATA THEFT, COMPUTER INTRUSIONS & RELATED

5 ways to make sure you aren't the next Wikileak

http://news.idg.no/cw/art.cfm?id=A481020B-1A64-6A71-CE806F2E7DD70189

Chris Knotts, VP of technology and innovation at Force 3
15.02.2011 kl 15:41 | Network World (US)

Here are five key tips to help your government agency or enterprise avoid being the source of the next Wikileak.

This vendor-written tech primer has been edited by Network World to eliminate product promotion, but readers should note it will likely favor the submitter's approach.

Government and intelligence officials around the globe have been caught off guard and in many cases embarrassed and compromised by disclosures of documents on the Web site WikiLeaks.
For security and IT professionals, these leaks serve as an important wake-up call to improve policies, procedures and safeguards. Here are five key tips to help your government agency or enterprise avoid being the source of the next Wikileak.

I. Security Policies and Procedures. Every government organization or enterprise must have policies in place to define who gets access to what information, and when. These policies and procedures must be actively maintained and updated and properly communicated. Then, the security policy can be administered by leveraging technology and putting the proper tools in place to secure, enforce, and mitigate risk to the organization.

In the October 2010 WikiLeaks case in involving some 400,000 U.S. military documents about the Iraq war, policy could have limited access to the systems that contained the sensitive information to those that had a "need to know." In highly sensitive information environments the policy should require strict management, monitoring and control of access only to people who have a legitimate need to know. Governance, Risk and Compliance (GRC) tools allow organizations to automate some aspects of this task by overlaying security policies and controls over corresponding data sources from switches, routers,

security platforms, servers, end points and applications, for a real-time view of their state of compliance.

However, no policy can be 100% effective, and many organizations will experience someone on the inside who has met the policy requirement, does have a legitimate need to know, but has illicit intentions. In these cases the security technology should provide the next layer of defense to meet these internal threats.

II. Implement Host-Based Security Solutions. Host-based security solutions include tools that allow an organization to protect and control laptops and desktop computers. Examples would be anti-virus/anti-malware products and software that prevents a user from using a USB drive or writable CD drive on a computer on a classified network.

Essentially, host-based security protects and limits what users can do at workstations. Host-based controls can disable, for example, simultaneous wired and wireless network capability, which can act as an entry point for a hacker. Host-based security solutions can also be integrated with network access control (NAC) systems to create a first line of defense for systems that regularly go on and off of the network, such as laptops. If a laptop is infected with a virus, or misses an important security patch while disconnected from the organization's network, the host-based security solutions, in conjunction with the NAC solutions, can assure that effected systems is quarantined, and cleaned of the virus, or receives the proper security patch before it is allowed onto the network.

III. Data Loss Prevention (DLP). DLP tools allow an organization to be aware of activity across the network. This includes monitoring what goes out of the network through e-mail, file sharing and via FTP. An organization can fine-tune the solution and have DLP watch the network for particular events, such as blocking e-mail that contains sourcecode or credit card or social security numbers.

IV. Traffic Profiling Tools. These tools can look across the network at individual users in aggregate and see what type of sites are being visited, with a particular emphasis on any sites that enable file-sharing, such as Dropbox, Mozy or YouSendIt. Network administrators may not want or need to block such sites, but it is helpful to know, in real time, when a user accesses these sites and for what purpose.

Profiling tools can also detect subversive attempts to extract data from a network. Every device on a network is expected to act a certain way when communicating. The network traffic to and from a printer should looks like a printer. If the traffic-profiling tool detects a printer looking more like a Linux

workstation, then someone may be trying to spoof the printers IP address for the purpose of exploiting a system of extracting data.

V. Log Management & Correlation. Almost every activity on a network leaves a "breadcrumb trail" in the form of log entries -- automated entries on the servicers and network devices that users interact with on a network. As a result, if an information leak does occur, logs will provide easier access to forensic information that can go back a few days or a few years. These tools can help determine the source of the leak more rapidly. Importantly, once the path that someone took to get data out of the network is identified, then new policies and procedures can be created to prevent a repeat occurrence.

When implemented in an enterprise environment, all of these individual solutions can be centrally managed and monitored. Most can be integrated with Security Incident and Event Management (SIEM) tools for a real-time "single pane of glass" view in the organization's security environment. SIEM tools allow organizations to automatically correlate events based on event "signatures" -- known combinations of events across multiple security platforms that have been know previously to constitute a breach, or attempted breach.

With experience, organizations can build their own signatures based on real or theorized threats in their own environment. Automated response to know events, such as persistent automated attacks -- attacks from botnet programs, or other coordinated automated attacks -- can allow an agency to move closer to a self-defending network.

Read more about wide area network in Network World's Wide Area Network section.

Blackhole-Powered Drive-By Download Attacks on the Rise

http://news.softpedia.com/news/Blackhole-Powered-Drive-By-Download-Attacks-on-the-Rise-184758.shtml

February 17th, 2011, 07:20 GMT| By Lucian Constantin

Researchers from cloud security provider Zscaler warn of an increase in the number of drive-by download attacks executed with the help of the Blackhole exploit toolkit.

Blackhole is a Russian Web attack hit similar to the more popular Eleonore or Phoenix kits. It features several different exploits that target Java, Adobe Reader and Windows vulnerabilities.

One of the author's selling points is the heavy obfuscation, which makes the exploits hard to detect for antivirus programs.

"Exploits crypt on special algorithms that make it impossible to code analysis and detection of anti-virus as well as services, Tipo wepawet and other counterparts," a line in the kit's description reads.

Its price is anything but cheap. A one-year license costs $1,500, a half-year one $700, while a three-month use will set a cybercriminal back $700.
These prices suggest that the return on investment for drive-by downloads is pretty high, otherwise paying so much for a single component of the attack would not be justified.

According to Zscaler researchers, a Google search for the URL pattern created by this kit on abused domains returns thousands of results.
A malicious .jar applet used by the Blackhole kit to exploit a 2009 Java vulnerability has a low detection rate on Virus Total at the moment and so does the infected executable it drops.

Other vulnerabilities exploited by this version are the 2010 Windows Help Center flaw and a Windows Media Player one targeted through malformed ASX files.
"We are [...] seeing large number of malicious domains hosting Blackhole exploits kit. [...] Even though the price of this exploit kit is high, it remains a sought after commodity," Zscaler security researcher Umesh Wanve, says.

Drive-by download attacks are one of the primary vectors of malware infection on the Internet. Thousands of legit Web pages are being compromised every day and have malicious code injected into them.

Users can protect themselves by having an up-to-date antivirus program installed, which is capable of monitoring and blocking Web traffic.

Flash drives dangerously hard to purge of sensitive data

When secure wiping isn't

http://www.theregister.co.uk/2011/02/21/flash_drive_erasing_peril/print.html

By Dan Goodin in San Francisco

Posted in Security, 21st February 2011 22:27 GMT

In research that has important findings for banks, businesses and security buffs everywhere, scientists have found that computer files stored on solid state drives are sometimes impossible to delete using traditional disk-erasure techniques. Even when the next-generation storage devices show that files have been deleted, as much as 75 percent of the data contained in them may still reside on the flash-based drives, according to the research, which is being presented this week [1] at the Usenix FAST 11 conference in California. In some cases, the SSDs, or sold-state drives, incorrectly indicate the files have been "securely erased" even though duplicate files remain in secondary locations.

The difficulty of reliably wiping SSDs stems from their radically different internal design. Traditional ATA and SCSI hard drives employ magnetizing materials to write contents to a physical location that's known as the LBA, or logical block address. SSDs, by contrast, use computer chips to store data digitally and employ an FTL, or flash translation layer, to manage the contents. When data is modified, the FTL frequently writes new files to a different location and updates its map to reflect the change.

In the process left-over data from the old file, which the authors refer to as digital remnants, remain.

"These differences between hard drives and SSDs potentially lead to a dangerous disconnect between user expectations and the drive's actual behavior," the scientists, from the University of California at San Diego, wrote in a 13-page paper. "An SSD's owner might apply a hard drive-centric sanitization technique under the misguided belief that it will render the data essentially irrecoverable. In truth, data may remain on the drive and require only moderate sophistication to extract."

Indeed, the researchers found that as much 67 percent of data stored in a file remained even after it was deleted from an SSD using the secure erase feature offered by Apple's Mac OS X. Other overwrite operations – which securely delete files by repeatedly rewriting the data stored in a particular disk location – failed by similarly large margins when used to erase a single file on an SSD.

Pseudorandom Data operations, for instance, allowed as much as 75 percent of data to remain, while the British HMG IS5 technique allowed as much as 58 percent.

Singling out one or more files to be erased is the only sanitization technique that allows the disk on which the data is stored to continue being used. And yet the researchers found that all single-file overwrite techniques failed to remove all digital remnants, even when the procedure was accompanied by disk defragmenting, which rearranges the remaining data in the file system.

"Our data shows that overwriting is ineffective and that the 'erase procedures provided by the manufacturer' may not work properly in all cases," the paper warns.

Whole-disk wiping techniques faired only slightly better with SSD media. In the most extreme case, one unnamed SSD model still stored 1 percent of its 1 GB of data even after 20 sequential overwrite passes on the entire device. Other drives were able to securely purge their contents after two passes, but most of them required from 58 hours to 121 hours for a single pass, making the technique unviable in most settings.

The researchers also found serious failures when subjecting SSD media to degaussing, in which a drive's low-level formatting is destroyed. Because degaussing attacks magnetism-based features of disks, it is ineffective when applied to next-generation storage devices. "In all cases, the data remained intact," the researchers wrote.

The researchers found the most effective way to sanitize data on SSDs was to use devices that encrypted their contents. Wiping happens by deleting the encryption keys from what's known as the key store, effectively ensuring that the data will remain encrypted forever.

"The danger, however, is that it relies on the controller to properly sanitize the internal storage location that holds the encryption key and any other derive values that might be useful in cryptanalysis," the researchers wrote. "Given the bugs we found in some implementations of secure erase commands, it is unduly optimistic to assume that SSD vendors will properly sanitize the key store. Furthermore, there is no way to verify that erasure has occurred (e.g., by dismantling the drive)."

The findings were recorded by writing files with identifiable patterns to SSDs and then using a field-programmable gate array device to search for the fingerprint after using secure erasure techniques to delete the files. The researchers' device cost about $1,000, but "a simpler, microcontroller-based version would cost as little as $200, and would require only a moderate amount of technical skill to construct," they said.

Right now, SSDs are most often encountered in USB thumb drives, and it's not unusual for them to hold as much as 32 GB of data. An increasing number of laptops by default ship with SSDs installed as the primary storage mechanism. Flash storage underpins that vast majority of smartphones, as well.

Smart cards no match for online spies

Robert McMillan

January 27, 2011 (IDG News Service)

http://www.computerworld.com/s/article/print/9206620/Smart_cards_no_match_for_online_spies?taxonomyName=Security&taxonomyId=17

The U.S. government has been stepping up its use of smart cards to help lock down its computer networks, but hackers have found ways around them.

Over the past 18 months, security consultancy Mandiant has come across several cases where determined attackers were able to get onto computers or networks that required both smart cards and passwords. In a report set to be released Thursday, Mandiant calls this technique a "smart card proxy."

The attack works in several steps. First, the criminals hack their way onto a PC. Often they'll do this by sending a specially crafted e-mail message to someone at the network they're trying to break into. The message will include an malicious attachment that, when opened, gives the hacker a foothold in the network.

After identifying the computers that have card readers, the bad guys install keystroke logging software on those computers to steal the password that is typically used in concert with the smart card.

Then they wait.

When the victim inserts the smart card into the hacked PC, the criminals then try to log into the server or network that requires the smart card for authentication. When the server asks for a digital token from the smart card, the bad guys simply redirect that request to the hacked system, and return it with the token and the previously stolen password.

This is similar to the techniques criminals have been using for several years now to get around the extra authentication technologies used in online banking.

Mandiant is the kind of company that businesses and government agencies call to clean up the mess after they've been hacked. It has done investigations at about 120 organizations overt the past year and a half. Most of them get hacked via a targeted e-mail. But in many cases, they were actually hacked years earlier, but never managed to remove the malicious software from their network, according to the report.

Companies or government agencies that assume that they are secure just because they use smart cards to authenticate, could be in for a nasty surprise some day, said Rob Lee, a director with Mandiant. "Everything is circumventable in the end," he said.

Robert McMillan covers computer security and general technology breaking news for The IDG News Service. Follow Robert on Twitter at @bobmcmillan. Robert's e-mail address is robert_mcmillan@idg.com

RSA 2011: Virtualization key to cloud security, Coviello says

http://www.csoonline.com/article/664925/rsa-2011-virtualization-key-to-cloud-security-coviello-says

In a keynote address at the RSA Security Conference here, RSA chief Art Coviello struck an optimistic tone about the future of security in cloud computing environments.

By Jaikumar Vijayan

February 15, 2011 — Computerworld —

SAN FRANCISCO -- Virtualization technologies can help enable better security and control in cloud computing environments, RSA chief Art Coviello said today. In a keynote address at the RSA Security Conference here, Coviello struck an optimistic tone on cloud security issues. While he acknowledged some of the concerns enterprises might have about moving data and applications to the cloud, he said that approaches to addressing any issues are closer than many think.

"Trust in the cloud is achievable today," Coviello said, adding that the key is to stop depending on security controls designed for physical infrastructures. Instead, companies need to be thinking about leveraging virtualization technologies to enable the enhanced security, visibility and control they want in cloud environments.

Coviello argued that security needs to be moved closer to the information and transactions it's protecting. In virtual environments, static perimeters give way to logical boundaries defined by information and transactions. As a result security needs to become logical as well.

"The IT stack is changing. Our boundaries are logical rather than physical. We can no longer depend on physical infrastructure for protection," he said. Virtual machines by nature are designed to dynamically adjust to workloads, he said. For security to really work in those kinds of environments, the controls need to be just as dynamic. "That means building security into virtualized components and, by extension, distributing security throughout the cloud," he said.

Security policies and best practices will need to be codified and enforced via automated security management systems for the cloud, Coviello said. The emphasis should be on enabling security that is more risk-based and adaptive to evolving conditions -- and less static.

The economics and agility enabled by cloud computing are pushing a growing number of companies to adopt it, regardless of the security and control concerns they may have, he said.

Counterintuitive as it may seem, "if leveraged properly, virtualization can be a pathway to surpassing the level of control and visibility that exists today in physical environments," he said.

As part of RSA's own effort to enable this sort of security, the company has launched a service called RSA Cloud Trust Authority , Coviello said. The service will leverage virtualization tools from VMware to deliver a set of identity management and compliance monitoring services in the cloud.

Jaikumar Vijayan covers data security and privacy issues, financial services security and e-voting for Computerworld. Follow Jaikumar on Twitter at @jaivijayan or subscribe to Jaikumar's RSS feed. His e-mail address is jvijayan@computerworld.com .

MARCH IN COUNTERINTELLIGENCE HISTORY

- March 4th, 1949: Soviet spy and DOJ employee Judith Coplon was arrested by FBI Agents as she attempted to pass classified information to U.N. Secretariat employee Valentin Gubitchev. Coplon was arrested based

on information derived from Venona, a program that decoded Soviet NKVD cables.

- March 6th, 1951: The trial of atom bomb spies Julius Rosenberg, Ethel Rosenberg, David Greenglass and Morton Sobell began on this date. They were convicted on 4/5/51. The Rosenberg's were given the death sentence; Sobell 20 years and Greenglass 15 years.
- March 10th, 1942: Because of a radio message sent by German spy Josef Jacob Johannes Starziczny, intercepted by FBI Agents stationed in Brazil during WWII, the Queen Mary was able to avoid German submarines and travel safely to England with its precious cargo of thousands of U.S. Soldiers. On this date, Starziczny was arrested by Brazilian police after being tipped off by FBI Agents.
- March 12th, 1941: FBI Director Hoover informed his Special Agents in Charge that the primary purpose of Japanese espionage was to determine the total strength of U.S. armed forces, and that the Japanese representatives in the U.S. had been cautioned that war between the U.S. and Japan was an eventuality.
- March 13th, 1942: Kurt Ludwig, a prolific Nazi spy in the U.S. in 1940 and 1941 was sentenced at trial to 20 years for his espionage activity. Eight other members of his spy ring were sentenced from five to 20 years.

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 (dates and location will be forthcoming).

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