EMPLOYEE

Security

CONNECTION

Volume 24 **A quarterly awareness briefing for defense industry and government employees** Number 2

In this issue. . .

Page

Russian Espionage: The Cold War Sequel

The recent case involving the arrest and deportation of the Russian intelligence network in the U.S. demonstrates that while the Cold War may have thawed, international espionage continues to thrive.

A brief recap: The U.S. recently sealed an agreement to trade 10 Russian agents (who'd just been arrested) for four men imprisoned in Russia for alleged contacts with Western intelligence agencies, bringing to a quick conclusion an episode that threatened to disrupt relations between the countries.

Long-term sleepers

The 10 long-term Russian sleeper agents all pleaded guilty to conspiracy before a federal judge after revealing their true identities. They were sentenced to time served, then transferred to Russian custody as part of a deal in which Moscow will release the four Russian prisoners, three of whom were serving long sentences after being convicted of treason for spying.

The swift end to the cases just 11 days after the Russians' arrests evoked memories of Cold War-style bargaining but underscored the new, often uneasy relationship between Washington and Moscow.

How'd it happen?

In a plot right out of a spy novel, the agents lived for more than a decade in American cities and suburbs from Seattle to New York, where they seemed to be ordinary couples working ordinary jobs.

But an FBI investigation that began at least seven years ago culminated with the arrests in Yonkers, Boston, and northern Virginia. U.S. authorities say the spies were part of what was called the "Illegals Program," an ambitious, long-term effort run by the S.V.R. (the successor to the Soviet K.G.B.) to plant Russian spies in the U.S. in order to gather information and recruit more agents.

The agents were directed to gather information on nuclear weapons, U.S. policy

ORED OFFICE OF RESEARCH AND ECONOMIC DEVELOPMENT
MISSISSIPPI STATE UNIVERSITY
Facility Security Office

toward Iran, CIA leadership, Congressional politics, and many other topics, prosecutors say. The Russian spies are known to have made contact with a former high-ranking national security official and a nuclear weapons researcher, among others.

Spy games

Criminal complaints related to the case include true hard-core espionage activities: spies swapping identical orange bags as they brush past one another in a train station stairway, an identity borrowed from a dead Canadian, forged passports, messages sent by shortwave burst transmission, the use of invisible ink, even a money cache buried for years in a field in upstate New York.

But the network also used cyber-age technology, according to the charges. They embedded coded texts in ordinary-looking images posted on the Internet, for example, and communicated by having two agents with laptops containing special software pass casually as messages flashed between them.

Experts on Russian intelligence expressed astonishment at the scale, longevity, and dedication of the program. They called it a return to the old days, but added that even in the most tension-filled years of the Cold War, there were probably fewer than 10 Soviet sleeper spies in the U.S.

Long-term spies put in place by the S.V.R. undergo training in an impressive array of techniques:

- Foreign languages, of course.
- Agent-to-agent communication.
- The use of codes and ciphers.
- The creation and use of a cover profession.
- Counter-surveillance measures.
- Avoiding detection (which doesn't always work, as the long-term investigation proves!).

Part of a trend

It's important to note that not everybody was surprised by the arrests. Many intelligence experts say espionage of all shades has actually increased since the Cold War, amplified by new technology and soaring demand for information in the public and private sectors.

Much of today's spying is conducted via computer, but secret agents like the ones recently deported still play a significant role in international spy games.

The corporate side

Moreover, spying isn't just the stuff of war and international politics. Espionage has become so ubiquitous in the corporate world, experts say, that billion-dollar merger-and-acquisition deals are almost never made without highly skilled spies getting involved.

Using some of the most sophisticated technology in the world, such as lasers that can record conversations from a mile away by picking up the slightest vibrations of an office window, the firms that handle this new-age corporate espionage are staffed almost entirely by former military and intelligence officials.

And as if competitors weren't enough to worry about, foreign nations do a vast amount of spying on U.S. companies. It's long been widely known that the Chinese in particular have an extremely elaborate intelligence network aimed at penetrating defense and technology firms.

After all, every piece of technology China steals is a piece the rapidly growing nation doesn't have to invent – or pay for. ❑

Trade Secrets Theft

With the "greening" of the U.S. economy, it shouldn't be surprising that the technology behind hybrid vehicles has become a prime target for corporate espionage artists – who may be stealing data for competitors or even nations.

A Michigan couple was recently charged with taking an estimated $40 million worth of hybrid-related trade secrets from General Motors, hoping to sell them to a GM competitor in China.

Shanshan Du and Yu Qin were indicted on conspiracy, fraud, and other charges. They had been under scrutiny for years; in fact, they were charged in 2006 with destroying documents sought by investigators, but that case was dropped while the broader probe was pursued.

Prosecutors say Du, who was hired at GM in 2000, purposely sought a transfer in 2003 to get access to hybrid technology and began copying documents by the end of that year. In 2005, she allegedly copied thousands of documents five days after getting a severance offer from the car maker.

By that summer, Qin was telling people he had a deal to provide hybrid technology to Chery Automobile, a GM competitor in China. The couple had set up their own company, Millennium Technology International.

China's rapid growth in manufacturing has led to an explosion of the nation's middle class, analysts say. With that explosion has come new demand for consumer goods such as autos. The expertise required to build marketable hybrid cars and trucks demands billions of dollars and years of development – and China's carmakers are thought to be seeking shortcuts.

Ex-Army Analyst Arrested

A former U.S. Army analyst who tried to board a flight to China with electronic files containing restricted Army documents was recently arrested and charged in federal court. Liangtian Yang, 26, of Lawton, Okla., is charged with one count of theft of government property. He became a U.S. citizen in 2006.

During a detention hearing, investigators testified he had copies of two restricted Army field manuals on multiple launch rocket systems on his computer equipment when he was arrested at Minneapolis-St. Paul International Airport. Yang had quit his job days earlier after he lost his security clearance for failing to report his marriage to a Chinese national.

The federal judge ordered Yang to remain in custody, agreeing with prosecutors that he was a flight risk. The FBI testified that Yang worked on experimental weapons. Along with the manuals on rocket systems, investigators found evidence indicating a classified document had once been on Yang's computer.

Scientist, Wife Charged in Nuclear Spy Sting

A former Los Alamos National Laboratory scientist and his wife have been indicted on charges alleging they passed weapons secrets to a person they believed was helping Venezuela develop a nuclear weapons program.

The FBI arrested the couple, Pedro Leonardo Mascheroni, 75, and Marjorie Roxby Mascheroni, 67, who recently made their initial appearance before a U.S. magistrate in Albuquerque. The Mascheronis face potential life prison sentences if convicted of all charges.

Pedro Mascheroni, a naturalized citizen and native of Argentina, worked in the LANL X Division from 1979 to 1988 when his security clearance was terminated; Marjorie Mascheroni was a technical writer and editor in the lab's Technology Transfer Section beginning in 1981.

Undercover sting

The 22-count indictment alleges Pedro Mascheroni met with an undercover FBI agent posing as a representative of the Venezuelan government. In the meeting, the scientist is said to have offered to sell nuclear and laser weapons to the county. His wife is accused of editing documents that were delivered to the undercover agent.

Pedro Mascheroni later claimed he was developing his own nuclear designs because he felt the U.S. weapons program was on the wrong track. He said he received $20,000 from the Venezuelan representative in an envelope he never opened.

He also said he planned to take the $800,000 promised to him to Congress in order to draw that body's attention to what he described as faulty weapons designs. Several security analysts have called that a preposterous excuse.

The indictment does not include a treason charge; instead, it accuses the couple of communicating restricted data, attempting to participate in the construction of an atomic weapon, conspiracy, and other charges.

According to U.S. Attorney Kenneth Gonzales, when the Mascheronis were hired at Los Alamos, they agreed to protect all classified information obtained from the labs.

He added that what the Mascheronis are accused of doing is very serious. "Our laws are designed to protect restricted data because in the wrong hands, it can potentially harm our national security," Gonzales said.

In recent years, Los Alamos has seen a number of embarrassing security breaches involving lost data, often due to careless employee use of laptops.

Economic Espionage

Kexue Huang, 45, was recently arrested and charged with economic espionage intended to benefit a foreign government. Huang was arrested in Westborough, Massachusetts, by FBI agents.

According to the indictment, he is a Chinese national who was granted legal permanent resident status in the U.S. Prosecutors say Huang, formerly of Carmel, Indiana, misappropriated and transported trade secrets and property to the People's Republic of China while working as a research scientist at Dow AgroSciences.

While employed at Dow, Huang allegedly directed university researchers in China to further develop the trade secrets. He is also said to have applied for grant funding used to develop the stolen secrets. "Economic espionage robs our businesses of hard-earned, protected research and is particularly harmful when the theft of these ideas is meant to benefit a foreign government," a prosecutor said.

SECURITYbriefs

Is Your Phone a Secret Spy?

It connects you to the world, but your cell phone could also be giving anyone from your boss to your spouse a window into your every move. The same technology that lets you stay in touch on the go can now let others tap into your private world – without you ever suspecting something is awry.

Most consumers know by now that newer phones include GPS data that makes it easy for others to tell where the phone is located.

And long gone are the days of simple wiretapping, when the worst your phone could do was let someone listen in on your conversations. The new generation of **cell phone spying** tools provides a lot more power.

All it takes is a two-minute software install, and someone can record your calls and monitor your text messages. They can even arrange to be automatically alerted when you dial a certain number, then instantly patched into your conversation. Anyone who can perform a basic Internet search can find the tools and figure out how to bug a cell phone in no time.

Here are the top five signs your cell phone may be bugged:

1. It's unusually warm even when you haven't been using it.
2. Battery life drops dramatically.
3. The screen flashes on and off for no reason you can explain.
4. Your monthly bill shows a surprising spike in SMS or data transmission activity.
5. You occasionally receive nonsense text messages.

The legality of these cell-spying tools is very sketchy; experts anticipate a series of lawsuits that will clarify the circumstances under which this software may be installed, but for now, the watchword is better safe than sorry.

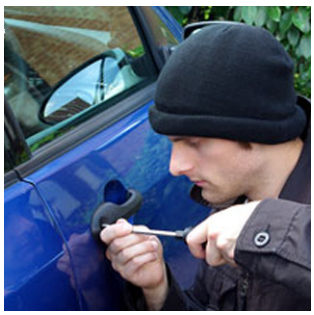
Cybercrime Stats

Here's an interesting look at some of the numbers found in a major new study of cybercrime in the U.S.:

- 34% of respondents say they cannot live without the Internet and must stay connected throughout the day.
- 40% of consumers say they are willing to share personal details with "brands, websites, and people they trust."
- 55% think cybercrime is a potential threat, and a full 27% "expect" to be scammed.
- 83% say they delete suspicious emails with attachments. (Good!)

10 Most Frequently Stolen Cars

Car buyers are leaning toward more economical models, but auto thieves apparently did not get the memo.



The Cadillac Escalade, a big luxury sport-utility vehicle, once the favorite of rappers and moguls, remains tops for average insurance theft losses, according to the Highway Loss Data Institute.

Escalade has topped the list for six of the past seven reports. Not only is the pricey vehicle targeted by thieves, but the average loss per vehicle stolen is among the highest, at $11,934. The institute says nearly one in four loss claims for the Escalade exceeded $40,000.

The top 10:

1. Cadillac Escalade
2. Ford F-250 crew
3. Infiniti G37
4. Dodge Charger HEMI
5. Chevrolet Corvette Z06
6. Hummer H2
7. Nissan Armada
8. Chevrolet Avalanche 1500
9. Chevrolet Silverado 1500 crew
10. GMC Yukon

Did You Know That. . .

… Spying by foreign governments to steal corporate information was the greatest concern identified by nearly 62% of the security experts who participated in a recent survey. The China/Asian region was singled out as the most likely suspect in such spying; closer to home, most respondents named lax employee behavior as the biggest domestic security threat.

… Nearly 50% of workers admitted that if they left an employer, they would take along some form of company property. Worse, sensitive data is high on the list of items they'd pilfer: 27% would take customer information, including contact info, while 23% would steal electronic files and 16% proprietary product information.

… A computer worm that targets critical infrastructure at companies doesn't just steal data – it leaves a back door that could be used to seize control of victimized businesses' computers. Stuxnet, which recently wreaked havoc worldwide, is being called a "serious development in the threat landscape" due to its ability to turn industrial computers into "zombies."

Beware of 'Free' Music Links

There's no such thing as a free lunch – or free tunes. Experts warn that computer users searching for free music may be opening themselves up to malware attacks.

According to new research, it may not be the names of popular music groups that pose a threat, as was previously thought, but rather searches with the words "free" and "downloads" that sharply raise the risk of a malware attack.

Here are some expert tips for avoiding the free-music blues:

- Avoid searching for "free" content. Instead, stick to legitimate, paid sites to get music and movies.
- Avoid clicking on links in banner ads on music, movie, and download sites that aren't well-established.
- Use comprehensive security software, updated regularly, to protect against the latest threats.
- Use common sense: Don't click on links posted in forums or on fan pages.
- Keep in mind that the more popular a topic, movie, or artist is, the more risky the search results will be.

More on freebies

Researchers found malware associated with a number of websites that advertise free downloads of sports games, movies, and TV shows. For example, 12% of sites that distribute unauthorized content are distributing malware, and 7% of sites offering unauthorized content have associations with cybercrime organizations.

Beware: these malicious sites often look very professional, experts warn. They typically lure users with the idea of a trial period, or sometimes a nominal fee that's much less than what may ultimately be charged.

Skimming Risk: Be on Your Guard

Here are four things experts say you should know about ATM "skimming," the practice of hacking bank machines to steal consumers' personal information:

ATM security is so poor worldwide that many more machines are likely to be easily compromised in the near future.

The bad guys are getting smarter and more sophisticated, experts warn. While older skimming devices were large, clunky, and easily identified by heads-up consumers, newer devices can fake out even experts.

While banks know there's a problem, and are working hard to address it, part of the issue is that they tend to refuse ATM access to "white-hat" hackers who might be able to help them identify their own weaknesses. These banks are (understandably) hesitant to let others know their security secrets.

Some ATMs in Eastern Europe localities have been infected with internal malware scripts that can capture users' details from within, without physical skimming props. And experts expect this trend to spread worldwide.

Fake Femme Fatale Fools Defense, Security Experts

A recent experiment that called for creating a fake social networking personality managed to snare even seasoned security veterans.

Robin Sage, according to her profiles on Facebook and other social-networking websites, was an attractive, flirtatious 25-year-old woman working as a "cyber threat analyst" at the U.S. Navy's Network Warfare Command. In less than a month, she amassed nearly 300 social-network connections among security specialists, military personnel, and staff at intelligence agencies and defense contractors.

One picture on her Facebook page showed her at a party posing in thigh-high knee socks and a skull-and-crossbones bikini captioned, "doing what I do best."

"Sorry to say, I'm not a Green Beret! Just a cute girl stopping by to say hey!" she rhymed on her Twitter page, concluding, "My life is about info sec all the way!"

And so it apparently was. She was also an avid user of LinkedIn, where her connections included men working for the nation's most senior military officer, the chairman of the Joint Chiefs of Staff, and for one of the most secret government agencies of all, the National Reconnaissance Office (NRO), which operates spy satellites.

Other friends included a senior intelligence official in the U.S. Marine Corps, the chief of staff for a U.S. congressman, and several senior executives at defense contractors.

Here's the problem: Robin Sage did not exist.

Honey trap!

The profile was a ruse set up by security consultants as part of an effort to expose weaknesses in the nation's defense and intelligence communities. To the embarrassment of many in the national security sphere, the trap worked beyond anybody's wildest expectations. Experts say the exercise reveals important vulnerabilities in the use of social networking by people in the national security field.

The fictitious Ms. Sage's connections invited her to speak at a private-sector security conference in Miami, and to review an important technical paper by a NASA researcher. Several invited her to dinner. And there were many invitations to apply for jobs.

"If I can ever be of assistance with job opportunities here at Lockheed Martin, don't hesitate to contact me, as I'm at your service," one executive at the company told her.

Military info

One soldier uploaded a picture of himself taken on patrol in Afghanistan; the shot's embedded data revealed his exact location. A defense contractor had misconfigured his profile so that it revealed the answers to the security questions on his personal email account.

Many other connections also inadvertently exposed personal data, including their home addresses and photos of their families – all important violations of operations and personal security, analysts point out.

Red flags

Those analysts added that they were surprised about the success of the effort, especially given that Ms. Sage's profile was bristling with what should have been red flags.

"Everything in her profile screamed 'fake,'" one expert said. For example, she claimed to have 10 years' experience in the cybersecurity field – which would mean she entered it at age 15 – and there is no such job as "cyber threat analyst" at the Naval Network Warfare Command. Even her name is taken from the code name of an annual U.S. special-forces military exercise, as a two-second Google search establishes.

Social Networking Not-To Do List

Don't use a weak password. Hackers who guess your password can use it to corrupt and misuse your account.

Don't reveal too much. Be careful about the information you disclose about your workplace or company.

Don't overlook privacy controls. You should understand and use these to control who sees what.

Don't click carelessly. Use caution when you click links that you receive in messages from your 'friends' on social networking sites.

Don't be too friendly. Beware of suspicious people adding you as a friend and watch out for the red flags.

Are You Exposing Your Organization to a Security Breach?

Most workers overestimate their own savvy when it comes to knowledge about risk and data breaches. To help you get a realistic portrait of your own expertise, here's a quiz to help you determine whether you're unwittingly exposing your employer to security trouble.

1. Do you use social networking websites?
   a. No.
   b. Yes, but only one.
   c. Yes, two to five.
   d. I use more than five social net works.

2. Do you post on blogs?
   a. No.
   b. Yes, one.
   c. Yes, two to five.
   d. I post on more than five blogs.

3. Do you post your resume to employment websites?
   a. No.
   b. Yes, I use one such site.
   c. Yes, two to five.
   d. I put my resume on more than five websites.

4. Do you post on bulletin boards and newsgroups?
   a. No.
   b. Yes, I post on one board or newsgroup.
   c. I post on two to five boards.
   d. I post regularly on more than five boards or newsgroups.

5. When you post online, do you:
   a. Use your real name? (Y/N)
   b. Post any military/government affiliations? (Y/N)
   c. Provide personal information? (Y/N)
   d. Hometown? (Y/N)
   e. Schools? (Y/N)
   f. Previous employment? (Y/N)
   g. Names of relatives? (Y/N)
   h. Names of friends? (Y/N)
   i. Training? (Y/N)
   j. Business associations? (Y/N)
   k. Personal associations? (Y/N)
   l. Post a daily journal of your activities? (Y/N)

6. Are you listed in yellow and/or white pages? (Y/N)
7. Do you have court records online? (Y/N)
8. Do you have real estate records online? (Y/N)
9. Do you have an online business? (Y/N)
10. Are you listed on school/university websites? (Y/N)
11. Are you listed on professional association websites? (Y/N)
12. Do you hold patents or copyrights? (Y/N)
13. Are you published? (Y/N)

Scoring

Now, go back and look at your answers, then assign a value from this scoring sheet:

- For each answer of a, you get 0 points.
- For each b, assign yourself 5.
- For each c, take a 10.
- For each d, take a big 25.
- Now assign yourself 5 points for each Yes answer.

You might have guessed by now that the goal in this quiz is a *low* score. Any number under 25 makes you the Invisible Man – congratulations, you are an extremely low risk! Scores of 25-45 tend to indicate workers who pose only a moderate risk, depending on other security related factors. A score higher than 50 means you may be compromising your own personal information, as well as sensitive data belonging to your employer.

Protect Yourself Online

To minimize your profile (and risk), consider these expert tips:

◆ Use tools to make your online use anonymous. You may want to seek out an "anonymizer," which is a tool that attempts to make activity on the Internet untraceable. It accesses the Internet on the user's behalf, protecting personal information by hiding the source computer's identifying information.

◆ Use generic free email accounts disposably.

◆ Use bogus "junk" information in web forms – that is, simply make up a name, address, phone number, and so on.

◆ Create random usernames.

◆ Use multiple usernames and email accounts so that all the websites you access cannot be linked together.

◆ If you have one, don't use your .mil or .gov email outside the Department of Defense network.

◆ Do not give out any personal information unless it's absolutely required for school, business, or professional transactions.

Why People Steal Secrets

Are you familiar with the case of Bradley Manning? He's the U.S. Army intelligence analyst who allegedly leaked reams of classified documents to Wikileaks, increasing the risk to his comrades in arms and making the country's war effort that much more difficult.

Why, many are asking, would a person do this? How *could* a person do this?

It turns out some answers may be found in a 20-year-old CIA study on moles. Project Slammer, as it was dubbed, now partially declassified, was based on extensive prison interviews with some 30 former military and intelligence personnel who'd been convicted of spying for Russia, China, and other hostile powers during the Cold War. Interviewees ranged from the lowest enlisted men to senior CIA officers like Aldrich Ames.

Seeking answers

The study sought to answer why these citizens had violated the trust their agencies had bestowed on them.

Two of the most important factors in a mole's decision to steal secrets were present in Manning's situation: the 22-year-old's alleged emotional distress, and lax military security. And keep in mind that security is everybody's job. Indeed, experts say co-workers may be best positioned to help avert acts of espionage and data leakage.

Counterintelligence experts say Americans who spy against the U.S. are increasingly motivated by ideology rather than by money, with nearly half of the known spies since the end of the Cold War showing allegiance to another country or cause. Prior to 1990, just a fifth of Americans spying for others were ideologically motivated.

The CIA study found conclusive evidence that behavioral changes are often associated with acts of espionage. Heavy drinking; drug dependence; signs of depression or stress; extramarital affairs; and divorce can all be warning signs of a security problem.

The report's authors believed, then and now, that if co-workers and bosses could be educated to intervene with a troubled employee early on, damaging espionage might be prevented.

Another trait common to moles, the experts say, is the belief that they're the smartest guy in the room. They enjoy the secret, the idea that they're included in sensitive discussions or work even as they betray those around them.

The bottom line is that personal demons drive people to leak, as well as to spy. And one of those demons can simply be a highly tuned, and highly selective, sense of moral outrage at certain kinds of government conduct.

Terrorism Trends

National security experts recently told members of Congress that the nature of terror threats to the U.S. is changing from foreign to domestic.

One emerging home-grown terrorism trend included in a new report is the once unthinkable threat of jihadist Americans launching suicide attacks within our borders.

Intelligence since 2001 suggests that while large, coordinated strikes are less likely now, the plans al-Qaida is pursuing may be even more difficult to detect and defeat. Experts say it's the "lone wolf" style of attack that's growing more likely.

The testimony revealed there are some benefits to these shifts in terrorist strategies. While lone-wolf attacks may be harder to detect, terrorists carrying them out are less likely to deploy large and devastating methods such as dirty bombs.

But not all of the testimony was positive. Americans need to be told that according to the law of averages, al-Qaida will successfully carry out a lone-wolf attack eventually, experts testified.

The Employee Security Connection (ISSN 0894-2080) is published quarterly by the National Security Institute, 116 Main Street, Suite 200, Medway, MA 02053. Subscriptions are $899 per year, telephone (508) 533-9099 for information concerning company/agency subscriptions.

October – December 2010