10 FEB 2012

(U) The FBI Tampa Division National Security Threat Awareness Monthly Bulletin provides a summary of previously reported US government press releases, publications, and news articles from wire services and news organizations relating to counterintelligence, cyber and terrorism threats. The information in this bulletin represents the views and opinions of the cited sources for each article, and the analyst comment is intended only to highlight items of interest to organizations in Florida. This bulletin is provided solely to inform our Domain partners of news items of interest, and does not represent FBI information.

In the FEBRUARY 2012 Issue:

<table>
<thead>
<tr>
<th>Article Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>NATIONAL SECURITY THREAT NEWS FROM GOVERNMENT AGENCIES:</td>
<td></td>
</tr>
<tr>
<td>White House Unveils New Strategy to Combat Homegrown Terror</td>
<td>p. 2</td>
</tr>
<tr>
<td>Chinese National Sentenced to Prison for Economic Espionage and Theft of Trade Secrets</td>
<td>p. 4</td>
</tr>
<tr>
<td>Research Chemist at New Jersey Pharmaceutical Company Pleads Guilty to Theft of Trade Secrets</td>
<td>p. 5</td>
</tr>
<tr>
<td>COUNTERINTELLIGENCE/ECONOMIC ESPIONAGE THREAT ITEMS FROM THE PRESS:</td>
<td></td>
</tr>
<tr>
<td>Former CIA Official Charged with Intelligence Leaks</td>
<td>p. 6</td>
</tr>
<tr>
<td>Canada Accuses Naval Officer of Sharing State Secrets</td>
<td>p. 7</td>
</tr>
<tr>
<td>Bradley Manning Case Signals US Vulnerability to 'Insider' Cyberattack</td>
<td>p. 8</td>
</tr>
<tr>
<td>US Arrests Iranian Scientist with Violating Export Laws by Buying High-Tech US Lab Equipment</td>
<td>p. 9</td>
</tr>
<tr>
<td>Kim Jong Il's Most Dangerous Legacy: A Thriving Nuclear-Export Business</td>
<td>p. 10</td>
</tr>
<tr>
<td>Federal Reserve Bank Contractor Arrested For Alleged Code Theft</td>
<td>p. 12</td>
</tr>
<tr>
<td>Motorola Accused of Trying to 'Destroy' Lemko Through 'Chinese Spy Ring' Insinuations</td>
<td>p. 12</td>
</tr>
<tr>
<td>Suspicion Grows China was Behind Hack of US Commission; Initially Linked to Indian Hackers</td>
<td>p. 14</td>
</tr>
<tr>
<td>United States Headed for Cyberwar Showdown with China in 2012</td>
<td>p. 16</td>
</tr>
<tr>
<td>China-Based Hacking of 760 Companies Shows Cyber Cold War</td>
<td>p. 17</td>
</tr>
<tr>
<td>CYBERSECURITY SPECIAL FOCUS FOR INDUSTRY</td>
<td></td>
</tr>
<tr>
<td>Cyber-Intruder Sparks Massive Federal Response, and Debate Over Dealing with Threats</td>
<td>p. 21</td>
</tr>
<tr>
<td>Top Ten Cybersecurity Stories of 2011</td>
<td>p. 26</td>
</tr>
<tr>
<td>CYBER THREAT ITEMS FROM THE PRESS:</td>
<td></td>
</tr>
<tr>
<td>Aggressive Phishing Attack Targets Military Personnel</td>
<td>p. 28</td>
</tr>
<tr>
<td>Security Trumps Secrecy in Cyber Fight, Prosecutor Says</td>
<td>p. 28</td>
</tr>
<tr>
<td>Anonymous Targets New York Officials and Companies</td>
<td>p. 29</td>
</tr>
<tr>
<td>US Shuts Megaupload.com, Hackers Retaliate</td>
<td>p. 31</td>
</tr>
<tr>
<td>Cybercrime is a Growing Threat for Government and Public Sector Organizations</td>
<td>p. 32</td>
</tr>
<tr>
<td>Viruses Stole City College of San Francisco Data for Years</td>
<td>p. 33</td>
</tr>
<tr>
<td>Victim Businesses Teaming Up To Fight Cybercriminals: Major Global Corporations Call for More Collaboration Among Organizations Hit by Cyberattacks</td>
<td>p. 34</td>
</tr>
<tr>
<td>Banks Unite To Battle Online Theft</td>
<td>p. 36</td>
</tr>
<tr>
<td>Malware Targets Bank Accounts; ‘Gameover’ Delivered Via Phishing E-Mails</td>
<td>p. 38</td>
</tr>
<tr>
<td>SEC Files Charges in Hacking Case</td>
<td>p. 39</td>
</tr>
<tr>
<td>Embedded Attacks and Emerging Targets to Dominate 2012 Security Landscape</td>
<td>p. 40</td>
</tr>
</tbody>
</table>
Hackers Expose Defense and Intelligence Officials in US and UK  p. 40
Cyber Spies Try Probing US Drone Plans  p. 42
Alleged Muscovite Cybercrime Daddy Hauled In To Face US Court  p. 43
10K Reasons to Worry About Critical Infrastructure  p. 44
Smart Grid Security Inadequate. Threats Abound  p. 45
SCADA Systems in Railways Vulnerable to Attack  p. 48

COUNTERTERRORISM THREAT ITEMS FROM THE PRESS:

Appeals Court Upholds Convictions in Fort Dix Plot  p. 49
Maryland Man Admits Plotting Terror Attack on Military Recruiting Center  p. 50
Muslim Man from Kosovo Charged in Florida Bomb Plot  p. 50
Colorado Man Arrested On Terrorism Charges  p. 53
Three Men Sentenced In North Carolina Terrorist Ring  p. 53
Feds Say Michigan Company Has Ties to Terrorist  p. 53
Analysis: Al Qaeda vs. the West: 2012 and Beyond  p. 55
Awlaki Video Urges US Muslims to Join Al Qaeda; Video Includes New English-Speaking Spokesman  p. 57
Former CIA Official: Al-Qaeda in Yemen Still Nimble  p. 58
Al Qaeda Affiliate Targets US Ships: Report  p. 59
Azerbaijan Arrests Plot Suspects, Cites Iran link  p. 59

(U) NATIONAL SECURITY THREAT NEWS FROM GOVERNMENT AGENCIES:

(U) White House Unveils New Strategy to Combat Homegrown Terror (USA Today, 08 DEC 201; National Public Radio, 08 DEC 2011)

(U) The United States has made significant progress in degrading al-Qaeda's capabilities in recent years—President Obama noted today that 22 of the top 30 al-Qaeda operatives have been killed or captured under his watch. Intelligence officials suspect the terror organization is increasingly focused on seeking US-born collaborators to carry out attacks. There have been 33 plots involving homegrown terrorists uncovered since 2009, according to the Senate Homeland Security and Government Affairs Committee.

"Protecting our nation's communities from violent extremist recruitment and radicalization is a top national security priority," according to the strategic document. "It is an effort that requires creativity, diligence and commitment to our fundamental rights and principles." The strategy draws broad outlines for fighting extremism and follows up on the White House's National Strategy for Counterterrorism, which was released in June. In a speech timed with the release of the counterterrorism strategy, Obama's top counterterrorism adviser, John Brennan, said the United States needed to avoid playing into al-Qaeda's strategy that "seeks to bleed us financially by drawing us into long, costly wars that also inflame anti-American sentiment." Brennan stressed that the White House would emphasize combating al-Qaeda's efforts to inspire people within the USA to carry out attacks on American soil.

(U) One interesting facet of the new document is a call for teaching local officials to recognize violent extremism. The strategy suggests federal and local authorities tweak the way they approach the American Muslim community on the issue. "Just as we engage and raise awareness to prevent gang violence, sexual offenses, school shootings and other acts of violence, so, too, must we ensure that our communities are empowered to recognize threats of violent extremism and understand the range of government and non-government resources that can help keep their families, friends and neighbors safe," the report says.
(U) New Partners

(U) The 20-page White House strategy, entitled "Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States", puts some meat on a bare-bones outline the administration released four months ago. In that August dispatch, the White House laid out broad initiatives for preventing the spread of violent extremism in the United States. That plan, just seven pages long, was criticized for being thin on details. The latest offering, which is expected to be released Thursday afternoon, is not exhaustive, but it provides a better idea of what the administration has in mind. The plan envisions a fusion of local partners, schools, community boards and leaders, with both local and federal law enforcement and other agencies.

(U) Many of these new partners, like the Department of Education, have never participated in national security issues before. "We had a long conversation about what kinds of things education can do," said a senior director of the National Security Council (NSC) at the White House, who spearheaded the initiative. "In the same way they fight gangs, or bullying, they can help here. The challenge is going to be trying to put the violent extremism initiatives into existing programs. But there are lots of ways to do it, and we'll work with the schools to tailor the approach to what they need."

(U) US counterterrorism officials have become adept at spotting terrorism suspects who travel overseas to get training or arrange large money transfers to support terrorist groups. But homegrown followers who quietly embrace violent extremism after watching al-Qaeda propaganda on their computers don't raise those same flags. In those cases, federal officials often learn about their intentions when it is too late. That's why the Obama administration is so eager to get into the fight local partners who are better positioned to pick up on these subtle cues.

(U) A UK Model

(U) The plan has some hints of a 2008 program in the United Kingdom called "Prevent." Authorities in the United Kingdom began dealing with homegrown terrorism long before it became an issue in the United States. The NSC senior director was in London studying the program for years before starting his job on the National Security Council in Washington. The Prevent program broke new ground in trying to get local officials and community leaders involved in spotting radicalization in its early stages. The program came in for some criticism, though; specifically, detractors said there wasn't enough separation between the community work officials were doing and the intelligence they ended up gathering. But Prevent has taught counterterrorism officials a lot about how to engage communities.

(U) Public Safety

(U) The new White House strategy is attempting to broaden the government's engagement with local communities across the board. If it works, the idea is to broaden the context of local discussions so they aren't just about terrorism; they are about something bigger. "We see what we're doing as a public safety issue," the NSC senior director said. "If a community was being targeted by gangs, the government would have some responsibility to help them. The same applies to a community that might be targeted with violent extremism; we have the same responsibility to help them. All parents are concerned about these kinds of issues, not just Muslim parents."

The strategy is posted at http://www.whitehouse.gov/sites/default/files/sip-final.pdf

(U) Kexue Huang, a Chinese national and a former resident of Carmel, Indiana, was sentenced today to 87 months in prison and three years of supervised release on charges of economic espionage to benefit components of the Chinese government and theft of trade secrets. The sentencing was announced by Assistant Attorney General Lanny A. Breuer of the Criminal Division, Assistant Attorney General for National Security Lisa O. Monaco, US Attorney Joseph H. Hogsett of the Southern District of Indiana, US Attorney B. Todd Jones of the District of Minnesota, and Robert J. Holley, Special Agent in Charge of the Indianapolis Field Office of the FBI. This is the first prosecution in Indiana for foreign economic espionage. Since its enactment in 1996, there have been a total of eight cases charged nationwide under the Economic Espionage Act.

(U) “Mr. Huang stole valuable trade secrets from two American companies and disseminated them to individuals in Germany and China,” said Assistant Attorney General Breuer. “Economic espionage and trade secret theft are serious crimes that, as today’s sentence shows, must be punished severely. Protecting trade secrets is vital to our nation’s economic success, and we will continue vigorously to enforce our trade secret and economic espionage statutes.” “The theft of American trade secrets for the benefit of China and other nations poses a continuing threat to our economic and national security,” said Lisa Monaco, Assistant Attorney General for National Security. “Today’s sentence demonstrates our commitment to detect, prosecute and hold accountable those engaged in these illegal activities.”

(U) “The Kexue Huang investigation and prosecution is an excellent example of how law enforcement and American corporations can work together to protect our corporations from economic espionage and the theft of extremely valuable trade secrets,” FBI Special Agent in Charge Holley stated. “Dow Agrosciences and the FBI cooperated extensively to make this important investigation a success. Economic espionage is a crime that undermines the competitiveness of our corporations and our national interest in protecting intellectual property. The FBI will continue to work collaboratively with the private sector to aggressively investigate those individuals that seek to harm our country’s economic interests by stealing our intellectual property and thereby undermining our competitive economic position in the world.”

(U) On Oct. 18, 2011, Huang pleaded guilty to one count of an indictment filed in the Southern District of Indiana for misappropriating and transporting trade secrets from Dow AgroSciences LLC with the intent to benefit components of the People’s Republic of China (PRC). Huang also pleaded guilty to one count of an indictment filed in the District of Minnesota for stealing a trade secret from a second company, Cargill Inc. According to court documents, from January 2003 until February 2008, Huang was employed as a research scientist at Dow, a leading international agricultural company based in Indianapolis that provides agrochemical and biotechnology products. In 2005, Huang became a research leader for Dow in strain development related to unique, proprietary organic insecticides marketed worldwide.

(U) As a Dow employee, Huang signed an agreement that outlined his obligations in handling confidential information, including trade secrets. The agreement prohibited him from disclosing any confidential information without Dow’s consent. Dow employed several layers of security to preserve and maintain confidentiality and to prevent unauthorized use or disclosure of its trade secrets. Huang admitted that during his employment at Dow, he misappropriated several Dow trade secrets. According to plea documents, from 2007 to 2010, Huang transferred and delivered the stolen Dow trade secrets to individuals in Germany and the PRC. With the assistance of these individuals, Huang used the stolen materials to conduct unauthorized research with the intent to benefit foreign universities that were tied to the PRC government. Huang also admitted that he pursued steps to develop and produce the
misappropriated Dow trade secrets in the PRC, including identifying manufacturing facilities in the PRC that would allow him to compete directly with Dow in the established organic pesticide market.

(U) According to court documents, after Huang left Dow, he was hired in March 2008 by Cargill, an international producer and marketer of food, agricultural, financial and industrial products and services. Huang worked as a biotechnologist for Cargill until July 2009 and signed a confidentiality agreement promising never to disclose any trade secrets or other confidential information of Cargill. Huang admitted that during his employment with Cargill, he stole one of the company’s trade secrets – a key component in the manufacture of a new food product, which he later disseminated to another person, specifically a student at Hunan Normal University in the PRC. In the plea agreement, Huang admitted that the aggregated loss from the misappropriated trade secrets exceeds $7 million but is less than $20 million.

(U) The sentence announced today is an example of the type of efforts being undertaken by the Department of Justice Task Force on Intellectual Property (IP Task Force). Attorney General Eric Holder created the IP Task Force to combat the growing number of domestic and international intellectual property crimes, protect the health and safety of American consumers, and safeguard the nation’s economic security against those who seek to profit illegally from American creativity, innovation and hard work. The IP Task Force seeks to strengthen intellectual property rights protection through heightened criminal and civil enforcement, greater coordination among federal, state and local law enforcement partners, and increased focus on international enforcement efforts, including reinforcing relationships with key foreign partners and US industry leaders.

(U) To learn more about the IP Task Force, go to www.justice.gov/dag/iptaskforce/.

(U) Research Chemist at Global Pharmaceutical Company in New Jersey Pleads Guilty to Theft of Trade Secrets (US Department of Justice Press Release, 17 JAN 2012)


(U) Sanofi is a global healthcare company with US headquarters in Bridgewater, New Jersey. It develops, manufactures and markets healthcare products including the prescription drugs Allegra, Plavix, Copaxone and Ambien. Li worked as a research scientist at Sanofi’s Bridgewater headquarters from August 2006 through June 2011, where she directly assisted in the development of a number of compounds that Sanofi viewed as potential building blocks for future drugs. These compounds were Sanofi’s trade secrets, and had not been disclosed outside of Sanofi in any manner, including by means of a patent application.

(U) While employed at Sanofi, Li was also a 50 percent partner in Abby, which is engaged in the sale and distribution of pharmaceuticals. Li admitted that between October 2008 and June 2011, she accessed an internal Sanofi database and downloaded information related to a number of Sanofi compounds, including their chemical structures, onto her Sanofi-issued laptop computer. She also admitted she then transferred the information to her personal home computer by sending it to her personal e-mail address or via a USB thumb drive. Li acknowledged that she made the stolen compounds available for sale on Abby’s website.
(U) The charge to which Li pleaded guilty carries a maximum potential penalty of 10 years in prison and a $250,000 fine. Sentencing is currently scheduled for April 23, 2012. US Attorney Fishman credited special agents of the FBI, under the direction of Special Agent in Charge Michael B. Ward, with the investigation.

(U) **Analyst Comment:** This case illustrates the threat to intellectual property from China and US-based subsidiaries of Chinese companies.

(U) **COUNTERINTELLIGENCE/ECONOMIC ESPIONAGE THREAT ITEMS FROM THE PRESS**

(U) **Former CIA Official Charged with IntelligenceLeaks** (AFP, 25 JAN 2012, ABC News, 25 JAN 2012)

(U) A former CIA official was charged in January with leaking classified information to journalists, including the name of a covert agent and the interrogation of a top Al-Qaeda operative, the Justice Department said. John Kiriakou, who served with the CIA between 1990 and 2004, was charged with violating a law that makes it illegal to disclose the identity of a covert officer, and lying to a CIA publications review board, the department said. Kiriakou is being charged on two counts of violating the Espionage Act and one count of violating the Intelligence Identities Protect Act, "for allegedly illegally disclosing the identity of a covert officer," the Justice Department statement said, according to CNN. The covert officer whose identity was allegedly divulged was described in this report. "Safeguarding classified information, including the identities of CIA officers involved in sensitive operations, is critical to keeping our intelligence officers safe and protecting our national security," Attorney General Eric Holder said. "Today's charges reinforce the Justice Department's commitment to hold accountable anyone who would violate the solemn duty not to disclose such sensitive information," he said in a statement.

(U) The Justice Department said the charges stem from an investigation into classified information that found its way into filings by defense lawyers representing detainees held at Guantanamo Bay, Cuba. It alleged that Kiriakou disclosed the identity of a covert CIA officer to a journalist in a pair of emails in July and August 2008, identifying him as a "team leader" of a certain operation. Kiriakou also was alleged to have provided information about a second CIA officer and his involvement in the capture and interrogation of Abu Zubaydah, an Al-Qaeda figure who was waterboarded during secret CIA interrogations. The Justice Department said he provided information about the CIA officer used in a New York Times story in June 2008 about the Abu Zubaydah case.

(U) One of the journalists in communication with Kiriakou allegedly passed the information about the second CIA officer to a Guantanamo defense counsel, which led to the officer being followed and photographed. Kiriakou also was alleged to have lied to a CIA review board in the course of seeking permission for publication of a book about his experiences called "The Reluctant Spy: My Secret Life in the CIA's War on Terror."

(U) A Canadian naval officer who worked in some of the country’s key military intelligence centers has been charged with breach of trust and passing along government secrets to a “foreign entity.” The officer, Sub-Lt. Jeffrey Paul Delisle, 40, remained in jail on Tuesday after his lawyer asked a court in Halifax, Nova Scotia, to delay a bail hearing to give him more time to study the government’s case. Neither the Royal Canadian Mounted Police, the military, nor the government offered much detail publicly about the charges, including the identity of the foreign power. But the Canadian television network CTV said it was Russia, without giving the source for that information.

(U) Court documents assert that the spying began four and a half years ago and continued until mid-January, when intelligence and police officials raided Lieutenant Delisle’s house in suburban Halifax. Until his arrest, Lieutenant Delisle worked at Trinity, an intelligence and communication center that is part of a large naval base in Halifax. A professor who teaches defense policy at the Graduate School of Public and International Affairs of the University of Ottawa, said Trinity was primarily responsible for tracking the position of military ships in the Atlantic Ocean, including submarines. According to several Canadian news reports, Lieutenant Delisle once worked in the main clearinghouse for military intelligence at the headquarters of the Department of National Defense in Ottawa, as well as its top operational planning unit in nearby Kingston, Ontario.

(U) Canada’s defense minister, Peter MacKay, would not answer questions about the possibility of Russia’s involvement. “I am not going to play Clue,” he told reporters in Ottawa, adding that despite the episode, “our allies have full confidence in Canada, full confidence in our information.” Officials of the Russian government would not comment. In a statement, Bob Paulson, the commissioner of the Royal Canadian Mounted Police, said the force was “not aware of any threat to public safety at this time from this situation.” Speaking hours after the police statement was released, however, Mr. MacKay said at a news conference that it was still too early to determine that. “Those are issues that will be determined in the future,” he told reporters.

(U) At the courthouse in Halifax, Lieutenant Delisle’s lawyer would not say how his client intended to plead to one charge of breach of trust under Canada’s criminal laws and two charges under the Security of Information Act. The lieutenant is the first person to be charged under the security law, which replaced an earlier Official Secrets Act and carries a maximum penalty of life in prison.

(U) An intelligence specialist at the Munk School of Global Affairs at the University of Toronto, said sub-lieutenant was a relatively low rank for a 40-year-old officer, suggesting that he had little career success. “That raises questions about career disappointment and revenge,” he said. Despite the government’s initial efforts to play down the seriousness of the arrest, the specialist said Lieutenant Delisle probably had access to a wide range of secrets given his job history. “The rank doesn’t matter,” he said. “The security clearance matters.” He and the University of Ottawa professor said the places where the lieutenant worked require high security clearances. Both men said Russia and China would be interested in the naval intelligence the lieutenant handled on a daily basis. It would include important data about American naval operations because of the close ties between the two navies.

(U) Spokesmen for the FBI, the CIA and the Justice Department in Washington all refused to comment on the case. The University of Ottawa professor said it was also possible that Iran, perhaps through an intermediary, might have used the officer to gain information about NATO naval movements near the Middle East. But if a major security breach has occurred, he said, Canada will most likely deal with the case as quietly as possible. “If it is a bigger issue,” he said, “the incentive will be for most governments to cover it over.”
UNCLASSIFIED

(U) Bradley Manning Case Signals US Vulnerability to 'Insider' Cyberattack (The Christian Science Monitor, 22 DEC 2011)

(U) The US government says Bradley Manning carried out a cyberattack from the inside, stealing thousands of secret US intelligence documents. Nearly half of US companies deal with similar cyberattacks each year, data suggest. At a time when nation-states and hacker-activists worldwide are increasingly infiltrating US networks to steal sensitive information, the allegations against Pfc. Bradley Manning highlight a cybersecurity threat that might be just as dangerous.

(U) In December Private Manning entered the seventh and perhaps final day of his pretrial hearing to determine whether he should be face a full court-martial on charges of stealing and leaking US intelligence to the WikiLeaks website. Among its accusations against Bradley, the US government says he walked out of a US military base in Iraq with a compact disc labeled "Lady Gaga" that actually held more than 251,000 secret State Department diplomatic cables. If true, the case shows the "insider" cyberthreat to companies, governments, and organizations. The attacks can range from disgruntled employees shutting down 1,000 company mobile phones at once to insiders changing computer codes to hide any records of money they have stolen.

(U) The trend lines for insider attacks are not as dramatic as those for outside attacks. Indeed, they have mostly held steady for a decade. But a 2011 survey found that nearly half of the organizations it polled reported an “insider incident” last year, suggesting the threat remains significant, and perhaps overlooked. "Companies today are going to greater lengths to keep outsiders and nation-states out of their networks, yet insiders come to work every day,” says the technical manager of the CERT Insider Threat Center, a division of the federally funded Software Engineering Institute at Carnegie Mellon University in Pittsburgh, Pa. “Most of these malicious insiders do what they do every day,” she adds. During the past decade CERT has documented more than 700 cases of insider cyberattacks by previously trusted people at the computerized heart of many organizations.

(U) The 2011 Cyber Security Watch Survey reported that 43 percent of 607 organizations queried reported an "insider incident" last year. That finding fits between the 2006 peak of 55 percent and the 2005 low of 39 percent. The report also suggested that insider attacks are in many cases more damaging than outsider attacks. One-third of respondents said they were more costly than other types of attack, whereas 38 percent said attacks by outsiders were more costly.

(U) Insider attacks break down to four main categories:

(U) • Sabotage of company computers

(U) • Theft of proprietary information

(U) • Release of sensitive data

(U) • Espionage

(U) The CERT technical manager has seen it all. One company's mobile devices were suddenly disabled for nearly 1,000 employees, grinding sales and delivery operations to a halt for days, she wrote in a June report. A network architect had programmed the cyber “bomb” to go off three months to the day after resigning after being demoted. In another instance, a company sued a former programmer who was discovered selling a competing product at a tradeshow. Investigators discovered copies of the company’s source code on his home computer, stolen on his last day of work there, the CERT report recounts.

UNCLASSIFIED
(U) Fraud is usually a longer-term, more subtle insider attack, she notes. A financial company’s audit discovered a $90,000 discrepancy in a software engineer's personal loan account. As it turns out, the employee had modified critical source code to siphon off money to cover fraudulent personal loans he had created. And the 700 cases documented by CERT are just the tip of the proverbial iceberg, since most cases never see the light of day.

(U) "I've learned about 71 major insider threat investigations over the last 12 years, none of which have become public to date," says the director of security services for White Badger Security, a security company in Breinigsville, Pa. "It's often the people in charge who are the problem. Network administrators in charge of the security systems of those companies accounted for about half of all those cases." Even social networks have become a security threat. "It's really a new vulnerability: Employees talking about products, big contracts, bragging to friends and family on these sites," says the co-director of the Intellectual Property Program at Suffolk University Law School in Boston. “Then it turns out to be a violation of a trade secret.”

(U) What's needed is a better awareness of how to lessen the risks, experts say. Restricting access is vital. The State Department has completely revised its access privileges in the wake of the Manning case. Many observers say he should never have been allowed access to documents he didn't need for his work. "Companies need to do a better job with basic security measures as simple as performing background checks on employees and limiting their access to highly sensitive information," says a trial lawyer and partner at Norris, McLaughlin & Marcus, specializing in technology law.

(U) Another easy step is monitoring the company computer network activities of fired or demoted employees for at least a month before and after they leave the company, the CERT technical director notes. Research has shown gains in automated monitoring to detect insider threats, the accessing of sensitive files by the wrong people or at the wrong time, for instance. But for now, humans are still the best detector. "Yes, the research is there and automated tools will emerge in due course," writes a researcher at the University of Buffalo. But today, a "completely automated tool doesn't exist."


(U) The United States has arrested and charged an Iranian semiconductor scientist with violating US export laws by buying high-tech US lab equipment, a development likely to further worsen Iranian-US tensions. Prison records show the United States is holding Seyed Mojtaba Atarodi, 54, a microchip expert and assistant professor at Tehran's prestigious Sharif University of Technology, in a federal facility in Dublin, Calif., outside San Francisco. The Iranian interest section in the Pakistani embassy in Washington said it was aware of the arrest.

(U) Atarodi arrived at a January bond hearing in federal district court in San Francisco wearing a green jump suit and politely bowed to his attorney. Before the hearing began, the judge closed the courtroom except to attorneys and members of the family. According to friends, Atarodi was detained Dec. 7 after stepping off a plane in Los Angeles. US law enforcement officials have declined to discuss any aspect of Atarodi’s case, and records indicate the charges have been sealed. But a Sharif University spokesman said he has been charged with buying instruments from the United States. The university official spoke only on condition of anonymity because of the potential repercussions of the case.
(U) The arrest comes as the United States, Israel and their allies are using diplomacy, sanctions and intelligence efforts to try to cripple what they suspect is Iran's drive to lay the foundations of a nuclear weapons program. Atarodi is listed as the author or coauthor of dozens of scientific papers dealing with microchip technology, though none appears to be explicitly related to military work. US officials in the past have targeted suspected export control violators dealing in so-called dual-use technology, which can have both civilian and military applications. The Sharif University spokesman said Atarodi was engaged only in civilian research. "The fact of the matter is that he was just a professor, and he was trying to buy some equipment for his lab, and the equipment was very, very simple, ridiculously simple stuff that anybody can buy," the spokesman said.

(U) After the end of the ten-minute hearing Thursday, Assistant US Attorney Philip Kearney declined comment. Abefa Atarodi, the scientist's brother, told The Associated Press: "The only thing we can tell you is that we care about him and are concerned with his health." He declined further comment. The arrest of an Iranian scientist in a US embargo case is rare, with most involving low-level middlemen living in the United States recruited to act as fronts for purchasers in Iran. But Iranian researchers in recent years have become central figures in the struggle between Tehran and the West over the country's extensive nuclear programs, which the International Atomic Energy Agency says has included arms-related research.

(U) At least four Iranian scientists have died under mysterious circumstances over about the past two years, and Israel is suspected of playing a role in the attacks. In the most recent incident, MostafaAhmadi Roshan, a chemist and official at Iran's Natanz uranium enrichment plant, was killed by a car bomb Jan. 11, reportedly while on his way to a memorial service for a scientist slain a year earlier. For years, Iran has insisted it is only interested in the peaceful uses of atomic energy and has resisted United Nation demands that it abandon its extensive uranium enrichment efforts. Enrichment technology can be used to make fuel for nuclear reactors or fissile material for bombs.

(U) The United States and Israel, meanwhile, are believed to have recruited Iranian scientists as agents or encouraged them to defect. Describing the problems faced by Iranian scientists visiting the United States, Hojabri cited an incident in 2006 when more than 50 researchers, executives and engineers from Iran headed for a forum on disaster management in Santa Clara, Calif., were detained and expelled after their arrival because their visas were revoked. The event was organized by a Sharif University alumni group.

(U) Analyst Comment: This article highlights the continued Iranian attempts to purchase or acquire all types of dual-use equipment in the United States to support their nuclear research program. Any company that manufactures or distributes dual-use medical devices or equipment, especially related to nuclear/radiological testing or measurement, or electronics components, should exercise extreme caution when dealing with new international customers, especially from the UAE, Hong Kong, Malaysia or Singapore. The FBI should be contacted after any suspicious contacts.


(U) Kim Jong Il's death leaves the Korean peninsula and the rest of East Asia in a period of great uncertainty. But one of Kim Jong Il's most dangerous legacies has security implications well beyond the region: he leaves behind a thriving nuclear weapons export business that must now be stopped. There has been mounting evidence in recent years that North Korea has set up an illicit nuclear export business to Syria, Iran and potentially elsewhere. Syria's Al-Kibar nuclear reactor, which was bombed by Israeli warplanes in 2007, closely resembled a North Korean facility used to produce plutonium for bombs, and one western diplomat told me that several senior North Korean technicians were killed in the raid.
(U) North Korea and Iran's sharing of technology for missiles that could be used to deliver nuclear warheads is so extensive that some analysts say it is only appropriate to view it as operationally a joint missile program. No one knows if North Korea is also helping Iran with nuclear weapons design, and it's possible it has other, yet-to-be-detected clients as well. North Korea shares little similarity or ideology with Syria or Iran; its dealings are largely profit-driven. For its clients, DPRK provides a black market to purchase sensitive nuclear technology without detection by the international community. The nightmare scenario is that Pyongyang would even sell fissile material -- the key ingredient for nuclear bombs -- to terrorists if the price is right. Most nonproliferation experts find this scenario unlikely as it would be quickest route imaginable to have your country bombed and possible invaded. However, the Syrian and Iranian cases show that DPRK has been happy to sell the technology needed to produce fissile material, and the missiles needed to deliver it What's not clear is how much this network relied on support or at least authorization from Kim Jong Il.

(U) But reports from North Korean defectors once involved in the tripartite proliferation network suggest it is highly sophisticated and involves many different layers of officialdom. It may work something like this: North Korean state trading companies working directly for the DPRK regime set up branch offices in mainland China. These companies contract private Chinese firms to send purchase orders to the local subsidiaries of European industrial machinery companies, who have set up shop in China specifically to cash in on China's growing domestic market. These domestic orders, of course, are not subject to export controls, so without knowing it, western subsidiaries sell dual-use technology, industrial tool and die equipment, for example, directly to private Chinese firms, who then use their established routes to transport the goods to North Korea. In terms of sales, North Korea state trading companies are also contracting private Chinese firms to move sensitive goods through Southeast Asia (including Myanmar) and on to clients in the Middle East.

(U) The success of this network is an unintended consequence of China's North Korea strategy, which has placed a high emphasis on a stable regime succession to Kim Jong Il's son, Kim Jong Un. The strategy is understandable: regime collapse in North Korea would send a flood of refugees across the border into some of the poorest provinces in China. Beijing may also believe that economic reform and party-to-party institution building can help reform North Korea and bring it in from the cold. Maybe so, but in the meantime this policy has created more opportunities for North Korea to increase its illicit activity through the mainland.

(U) Unfortunately, enlisting China's help in cracking down on the use of private Chinese firms by North Korean entities -- even now that Kim Jong Il is dead -- is a lost cause for the United States and its allies. China's port security and trade monitoring resources are woefully unmatched by the volume of trade in China today. Even more importantly, corruption at local levels is still a major problem. The Proliferation Security Initiative, launched in 2003 as a voluntary organization of nations cooperating to prevent the shipment of proliferation-sensitive technologies, has proven to be an increasingly effective tool for combating North Korean smuggling. It has led to the interdiction of several North Korean shipments of missile and WMD components, most recently the turning around by the US Navy of a Belize-flagged North Korean Vessel in June suspected of transporting missile technology on its way to Myanmar (and then on possibly to the Middle East). In the short term, the PSI should be continued. What's more, we should encourage PSI states -- and China -- to offer monetary rewards that lead to the interdiction of North Korean consignments. Mercenary traders, after all, can often be bought when they cannot be stopped.
North Korea is a backward, broken country with a dysfunctional economy. But its leaders are expert survivors and remarkably apt at getting what they need; we should not assume that this will change with Kim Jong Il’s passing. With two nuclear weapons tests already complete, North Korea has clearly learned how to construct a black market, full-service nuclear weapons program. There is growing evidence that they will now help any country that can pay to do the same. The death of Kim Jong Il should focus the West's attention on stopping the spread of North Korean technology. Cutting off the supply would buy us time to fight the other half of the battle. In countries and regions where the demand for nuclear weapons remains strong, we must do more to address the underlying issues that cause countries to seek nuclear weapons in the first place.

Analyst Comment: As this article notes, North Korea is using Chinese firms to contact western manufacturers of dual-use technology, such as industrial doe and die machinery, and purchase equipment in China for shipping to North Korea. Florida manufacturers and distributors of this type of equipment should conduct thorough due diligence when selling to new customers in China.

Federal Reserve Bank Contractor Arrested For Alleged Code Theft: Suspect Admitted to Stealing US Treasury Dept.-Owned Program (Dark Reading, 20 JAN 2012)

A government contractor is in custody for allegedly stealing proprietary software code from the Federal Reserve Bank of New York. The FBI and US Attorney for the Southern District of New York yesterday announced that Bo Zhang, 32, of Queens, N.Y., admitted to stealing the Government-Wide Accounting and Reporting Program (GWA) from the bank in July 2011 while he worked there as a contractor developing a piece of the GWA source code. He allegedly copied the GWA code onto an external hard drive owned by the bank and used it in a private computer programming training business.

“As today’s case demonstrates, our cyber infrastructure is vulnerable not only to cybercriminals and hackers, but also alleged thieves like Bo Zhang who used his position as a contract employee to steal government intellectual property. Fighting cyber crime is one of the top priorities of this office and we will aggressively pursue anyone who puts our computer security at risk,” said Manhattan US Attorney Preet Bharara in a statement. And FBI assistant director in charge Janice K. Fedarcyk said in a statement: “Zhang took advantage of the access that came with his trusted position to steal highly sensitive proprietary software. His intentions with regard to that software are immaterial. Stealing it and copying it threatened the security of vitally important source code.”

The $9.5 million GWA software application is owned by the US Treasury Department, and tracks US government finances. It handles ledger accounting within Treasury and account statements to federal agency bank customers. The source code is housed in “an access-controlled” database at the Federal Reserve Board of New York, where it’s under further development by the bank, according to the DOJ. If convicted, Zhang could face a maximum prison sentence of 10 years, up to three years of supervised release, and up to $250,000 in fines.

Motorola Accused of Trying to 'Destroy' Lemko Through 'Chinese Spy Ring' Insinuations (Network World, 08 NOV 2011)

The 4G cellular technology manufacturer Lemko Corp. sued Motorola Solutions and its lawyers in November, 2011, saying Motorola's claims that Lemko is allegedly part of a Chinese spy ring tied to the Chinese government and Chinese companies have unfairly damaged its business. The Schaumberg, Ill.-based privately held company, with Nicholas Labun its CEO and Shaowei Pan as chief technology officer, charge that Motorola and its lawyers have falsely claimed that Lemko employees are part of “a
Chinese spy ring," and that the intent in saying this is to "drive Lemko out of business by harassing its customers and suppliers" in order to end by "coercing the transfer of Lemko's patents and future technology to Motorola."

(U) The Lemko lawsuit, which also accuses Motorola of racial profiling of people of Chinese descent, is the latest in an ongoing three-year legal battle between the two companies that has as its starting point the former Motorola software engineer Hanjuan Jin, who in 2007 was arrested at Chicago O'Hare Airport by US Customs as she sought to board a plane to China. Jin, a US citizen born in China, was detained at O'Hare as she was ready to board a flight to China with a one-way ticket. She was found to be carrying $30,000 and more than 1,000 electronic paper documents from her former employer, Motorola, as well as Chinese documents for military telecommunications technology, according to the FBI affidavit filed in court.

(U) Jin, who is on trial in Chicago, stands accused by federal prosecutors of stealing mobile telecommunications technology for the benefit of China's military and a Beijing business, Kai Sun News (Beijing) Technology Company, also called SunKaisens. She has pled innocent. Motorola's own investigation into Hanjuan Jin's activities led the company to believe that Jin allegedly went to work for Lemko during a period she was ostensibly on medical leave from Motorola. In Motorola's civil lawsuit against Jin, Lemko as well as a handful of engineers of Chinese descent who worked for both companies at various points, Motorola in 2009 claimed that Jin "installed Motorola's proprietary secure virtual network ('VPN') access software on a Lemko-owned computer, accessed Motorola's protected computers through Motorola's secure VPN from a Lemko-owned computer and accessed Lemko's webmail system from Motorola's computers," while also getting "unauthorized access to Motorola source code and other valuable Motorola proprietary trade secrets and confidential information."

(U) In its lawsuit accusing Motorola of "abuse" and "unfair competition," Lemko largely defends Jin, who stands accused of economic espionage. "In fact, she was travelling to China to visit her family and was carrying with her what she believed were materials needed for her off-site work as a Motorola employee," the Lemko lawsuit contends. Lemko accuses Motorola of a "witch hunt" after the arrest of Jin, and that "Motorola falsely claimed that Lemko and Jin conspired to smuggle Motorola's trade secrets and other proprietary documents to China." Lemko accuses Motorola, and its corporate counsel Jeffrey Johnson along with Nixon Peabody law firm counsel Mark Halligan and Deanna Swits, of all being out to "destroy" Pan, Lemko's CTO, at Lemko, as well as CEO Labun, and drive Lemko out of business in the ongoing legal battle that has already lasted more than three years.

(U) The Lemko lawsuit filed in early November says Motorola and its lawyers "have used subpoenas twice served on more than 60 of Lemko's customers, suppliers and potential investors to discourage them from doing business with Lemko." Lemko says this is "causing them all to either cease doing business with Lemko or altering the business that was being done." "They have attempted to cast Lemko, Mr. Labun and Dr. Pan in an adverse light, disparaging their business and professional reputations and encouraging others to call them Chinese spies. They have also discouraged the United States Government from doing business with Lemko, resulting in the loss of a $200 million contract and future opportunities valued at $1 billion," the Lemko lawsuit filed yesterday states.

(U) Lemko also makes an accusation against Motorola in relation to China-based Huawei Technologies. "Motorola also directly interfered with the business relationship Lemko had with its supplier Huawei by telling Huawei that, if it did do business with Lemko, Dr. Pan or Mr. Labun, Motorola would not allow Huawei to bid on the possible sale of Motorola assets Huawei wanted to purchase. This, in effect, disrupted Lemko's ability to purchase needed equipment and products from Huawei at a critical time in Lemko's evolution." Lemko calls all of this a "misuse of the legal process" with the intent of destroying
Lemko and "coercing the transfer of Lemko's patents to Motorola, of obtaining Lemko's valuable technology."

(U) Lemko claims Motorola lawyers have falsely tied the firm to the Hanjuan Jin spy case, as a "smuggler of documents to China and as part of a Chinese spy ring." Lemko calls Pan, who went to university in Beijing and went to work for Motorola in the United States before joining Lemko, "one of the most prolific inventors in the history of Motorola, creating inventions that resulted in more than 60 patents now owned by Motorola. Unfortunately, like others of Chinese descent who worked at Motorola, Dr. Pan was racially profiled by Motorola's management team, including Johnson, and, as a result of that profiling and outright prejudice, labeled a spy for the Chinese government and for Chinese companies and a smuggler of documents and technology to China." Lemko says Motorola ultimately wants to get hold of cellular network technology that Pan developed at Lemko.

(U) Motorola Solutions indicated it will fight the accusations hurled by Lemko in its lawsuit. Motorola Solutions vice president of global communications, said, "We consider the allegations frivolous," and Motorola will "vigorously defend" itself against what it regards as "meritless claims." "Lemko's latest litigation tactic doesn't change Motorola Solutions' longstanding belief in the importance of protecting its intellectual property," he said.

(U) Suspicion Grows China was Behind Hack of US Commission; Initially Linked to Indian Hackers (Reuters, 18 JAN 2012; Reuters, 11 JAN 2012)

(U) Suspicion is growing that operatives in China, rather than India, were behind the hacking of emails of an official US commission that monitors relations between the United States and China, US officials said in January. News of the hacking of the US-China Economic and Security Review Commission surfaced earlier this month when an amateur "hacktivist" group purporting to operate in India published what it said was a memo from an Indian Military Intelligence unit to which extracts from commission emails were attached.

(U) But US officials who spoke to Reuters on condition of anonymity said the roundabout way the commission's emails were obtained strongly suggests the intrusion originated in China, possibly by amateurs, and not from India's spy service. A large cache of raw email data from the security breach, reviewed by Reuters, indicates that the principal target of the intruders was not the commission, but instead a Washington-based non-governmental pro-trade group called the National Foreign Trade Council (NFTC). The trade council is headed by William Reinsch, a former top US Commerce Department official who until recently served as the US-China Commission's chairman.

(U) A large proportion of the raw email traffic downloaded by the hackers consists of messages to and from Reinsch at his NFTC email address. Many of the emails were spam, but some related to the work of the commission, which was set up by Congress to take a critical look at a wide range of US dealings with China.

(U) Reinsch told Reuters that the NFTC first became aware in November that large quantities of its message traffic had been hacked. He said that law enforcement authorities, including the FBI, had been quickly notified. The FBI has declined comment. Reinsch said he could think of "no particular reason" why the Indian government or Indian hackers would be interested in him. By contrast, he and several other US officials said that Chinese hackers, whether amateur or directly affiliated with Chinese government, would have great interest in the US-China Commission's activities, both public and private.
(U) Soft Target

Sources familiar with the hacking and the related investigation said they draw two inferences from the fact that the principal target of the hack appears to have been Reinsch's email account at NFTC. First, the sources said they found it difficult to believe anyone connected with India would have taken the time or effort to track down Reinsch or his NFTC account, whereas his chairmanship of the US-China Commission made him a potential major target for Chinese hackers. Second, said the sources, the fact that Reinsch’s NFTC emails were the principal target suggests that whoever hacked them was hunting for a soft target with poor cyber-security. This suggests the hackers were amateurs rather than a foreign spy service.

Pinning down the origin and perpetrator of a particular cyber-intrusion can be fiendishly difficult, if not impossible, as hackers frequently take steps to mask their identity or appear that they are from a third country. One official familiar with the matter said that it was possible that all the hacked email traffic, including messages related to the US-China Commission, originated with the NFTC. Under this scenario, the reason commission traffic was included in the hacked material was that it consisted of copies of commission messages which were sent to Reinsch at his NFTC email address. But other officials said it was also still possible some emails were stolen directly from the commission or private email accounts of other commissioners.

A person familiar with details of the incident and related investigation said the hacked emails spanned a six-month period from late March to late October last year. The source said that about 85 percent of the traffic consisted of emails incoming to the NFTC, with the other 15 percent being outgoing messages from NFTC's server. The source said that there were significant gaps in the hacked traffic, covering both day-long and week-long periods, bolstering the notion the hacking was done by amateurs. Investigators are still trying to determine if the hacker successfully targeted NFTC's local network or a network which fed messages to a mobile device used by Reinsch.

(U) Indian Memo

The memo that triggered the investigation into a possible cyber-attack by Indian military intelligence is probably a fake, but it is clear from leaked documents that serious security breaches did take place. A little-known hacker group, "Lords of Dharmaraja," began posting the documents last year, but only drew widespread attention after the anti-virus software firm Symantec confirmed that a segment of its source code had been accessed by the group. Reuters has obtained a large digital cache appearing to contain emails that were posted by the group but were quickly blocked by file-sharing sites.

Dated between April and October last year, many of the emails were addressed to Bill Reinsch, a member of an official US commission monitoring economic and security ties between the United States and China, including cyber-security issues. Military and cyber-security experts in India say the hackers may have created the purported military intelligence memo simply to draw attention to their work, or to taint relations between close allies India and the United States.

The purported Indian intelligence memo implied that the commission emails had somehow been hacked using know-how supplied to the Indian government by mobile phone companies who, as payback, were afforded greater access to the Indian market. One of the mobile phone manufactures named in the purported memo, Apple, denied giving the Indian government backdoor access to its products. A second, Research in Motion, said the company does not typically comment on rumor or speculation, and a third manufacturer, Nokia, declined to comment. Indian government officials and agencies declined repeated requests for comment on the alleged government document, although some former Indian officials labeled the memo a fabrication. Two US officials familiar with the hacking incident said they were puzzled why
India would go to the trouble of hacking emails related to the US-China Commission, since its work had little if anything to do with India, and Indian officials and diplomats had never showed much interest in its activities.

(U) By contrast, the commission has been a regular target for what officials describe as persistent attempted hacking intrusions, many through the technique of "phishing," which involves sending bogus but convincing emails which purport to come from insiders but contain malicious code. Investigators strongly suspect these intrusions were launched by people from, or operating on behalf of, China. A large proportion of the hacked traffic examined by Reuters appeared to be what could be categorized as spam, including summaries of news articles and political fundraising pitches. Some hacked traffic from the US-China Commission had potentially sensitive implications, however, including messages in which commission personnel discuss matters under deliberation by the organization. These issues included the commission's attitude toward alleged Chinese theft of intellectual property and congressional deliberations about alleged Chinese currency manipulation.

(U) US officials said there was no indication hackers managed to gain access to electronic files related to the commission's most sensitive project, a classified version of its annual public report. Electronic materials related to this project are kept on classified servers, isolated from the Internet, which are operated by agencies other than the commission itself, one official said.

(U) United States Headed for Cyberwar Showdown with China in 2012 (Forbes, 22 DEC 2011)

(U) The new year is likely to bring a distinct shift in US national security priorities, as the Obama Administration and Congress sharpen their response to China's continuous assault on US information networks. Although intelligence-community analysts believe the most sophisticated intrusions are being executed by a relatively small number of agents linked to the general staff of China's People’s Liberation Army, the damage they are inflicting on US security and economic competitiveness is judged to be extensive.

(U) Thus far, China's cyber campaign consists mainly of espionage aimed at stealing military secrets and intellectual property. However, Gen. Keith Alexander, head of the Pentagon's joint Cyber Command established to counter such campaigns, said in November that, "We see a disturbing track from exploitation to disruption to destruction." Alexander wasn't talking just about the Chinese, but there's little doubt among intelligence analysts that Beijing is the biggest and most persistent perpetrator of cyber crimes.

(U) The question is what to do about it. To date, US cyber efforts have been focused mainly on defensive measures, seeking to repel network intruders in a fashion that Alexander likens to the famously failed Maginot Line. The National Security Agency and other US security organizations are known to have developed their own networkattack capabilities, but former White House cyber-security advisor Richard Clarke has warned that it would be dangerous for the United States to step up its own campaign against Chinese networks while US safeguards against retaliation are so weak.

(U) Under the leadership of a few forward-thinking policymakers such as former Deputy Secretary of Defense William Lynn, the Department of Defense and intelligence community have greatly strengthened their information defenses and begun helping industry to protect critical infrastructure. But insiders say the asymmetries between US and Chinese society make it hard to cope with China's cyber onslaught. Not only is America a much more open and porous place, but US agencies and private companies have a lot more information that's worth stealing.
(U) The United States is also well ahead of most other countries in moving both its security apparatus and commercial economy onto the Internet, which was not designed with security in mind. Cyber experts say that Internet operations are intrinsically vulnerable to attacks by the kind of highly-skilled agents that China's government employs, a problem that may be exacerbated as economic forces pressure federal agencies and corporations to outsource information resources to "the cloud." Not only is it easy to conceal the source of cyber attacks, but the Internet crisscrosses political boundaries in a manner that greatly diminished the effectiveness of traditional law enforcement techniques. As one former intelligence official told me, "If I think China is attacking me but it's using the server for the Chicago municipal hospital system, what am I supposed to do – take down the server?"

(U) Beyond issues of attribution and extraterritoriality, there is the simple reality that digital technology permits the compression of vast amounts of information into brief bursts of computer code. US officials speak of "terabytes" of information being stolen before intrusion was noticed, without any indication of where it went or how it might be exploited. And while there is seldom a "smoking gun" that points to a particular Chinese perpetrator, it's hard not to draw the obvious conclusion from the way the volume of cyber attacks drops off during the Chinese New Year holiday.

(U) China-Based Hacking of 760 Companies Shows Cyber Cold War (Bloomberg, 14 DEC 2011)

(U) Google Inc. and Intel Corp. were logical targets for China-based hackers, given the solid-gold intellectual property data stored in their computers. An attack by cyber spies on iBahn, a provider of Internet services to hotels, takes some explaining. iBahn provides broadband business and entertainment access to guests of Marriott International Inc. and other hotel chains, including multinational companies that hold meetings on site. Breaking into iBahn’s networks, according to a senior US intelligence official familiar with the matter, may have let hackers see millions of confidential e-mails, even encrypted ones, as executives from Dubai to New York reported back on everything from new product development to merger negotiations. More worrisome, hackers might have used iBahn’s system as a launching pad into corporate networks that are connected to it, using traveling employees to create a backdoor to company secrets, said the head of Trustwave Corp.’s SpiderLabs, a security firm.

(U) The hackers’ interest in companies as small as Salt Lake City-based iBahn illustrates the breadth of China’s spying against firms in the United States and elsewhere. The networks of at least 760 companies, research universities, Internet service providers and government agencies were hit over the last decade by the same elite group of China-based cyber spies. The companies, including firms such as Research in Motion Ltd. (RIM) and Boston Scientific Corp., range from some of the largest corporations to niche innovators in sectors like aerospace, semiconductors, pharmaceuticals and biotechnology, according to intelligence data obtained by Bloomberg News.

(U) ‘Stealing Everything’

(U) “They are stealing everything that isn’t bolted down, and it’s getting exponentially worse,” said Representative Mike Rogers, a Michigan Republican who is chairman of the Permanent Select Committee on Intelligence. China has made industrial espionage an integral part of its economic policy, stealing company secrets to help it leapfrog over the United States and other foreign competitors to further its goal of becoming the world’s largest economy, US intelligence officials have concluded in a report released in November. “What has been happening over the course of the last five years is that China, let’s call it for what it is, has been hacking its way into every corporation it can find listed in Dun & Bradstreet,” said Richard Clarke, former special adviser on cybersecurity to US President George W. Bush, at an October conference on network security. “Every corporation in the United States, every corporation in Asia, every
corporation in Germany. And using a vacuum cleaner to suck data out in terabytes and petabytes. I don’t think you can overstate the damage to this country that has already been done.”

(U) Foreign Governments

(U) In contrast, US cyberspies go after foreign governments and foreign military and terrorist groups, Clarke said. “We are going after things to defend ourselves against future attacks,” he said. Such accusations intensified when a November 3 report by 14 US intelligence agencies fingered China as the No. 1 hacker threat to US firms. While the Obama administration took the unprecedented step of outing China by name, the White House, US intelligence agencies and members of Congress are struggling to assess how much damage is being done during such attacks and what to do to stop them beyond public rebuke.

(U) For now, the administration is concentrating on raising awareness among company executives and seeking a commitment to improve security against such attacks. Rogers has a bill pending in the House that would permit the government to share secret information that would help companies spot hacker intrusions, such as signatures of malicious Chinese software.

(U) Consistently Denied Responsibility

(U) China has consistently denied it has any responsibility for hacking that originated from servers on its soil. Geng Shuang, a spokesman for the Chinese embassy in Washington, didn’t respond to several e-mails and phone calls requesting comment. Wang Baodong, another Chinese government spokesman in Washington, also didn’t respond to requests for comment. Based on what is known of attacks from China, Russia and other countries, a declassified estimate of the value of the blueprints, chemical formulas and other material stolen from US corporate computers in the last year reached almost $500 billion, said Rogers, a former agent for the Federal Bureau of Investigation.

(U) Stolen Information

(U) US officials are grappling with how stolen information is being used, said an economist and director of the US Cyber Consequences Unit, a non-profit research institute. Calculating the damage depends on hard-to-know variables, such as how effectively and quickly thieves can integrate stolen data into competing products, the senior intelligence official said. While a precise dollar figure for damage is elusive, the overall magnitude of the attacks is not, said the economist. “We’re talking about stealing entire industries,” he said. “This may be the biggest transfer of wealth in a short period of time that the world has ever seen.”

(U) The public evidence against China now being rolled out by the Obama administration, Rogers and others in Congress has been collected by the intelligence community over several years. Many of the details remain classified. The hackers who attacked iBahn are among the most skilled of at least 17 China-based spying operations the US intelligence community has identified, according to a private security official briefed on the matter who asked not to be identified because of the subject’s sensitivity.
(U) Massive Espionage Ring

(U) The hackers are part of a massive espionage ring specializing in infiltrating networks using phishing e-mails laden with spyware, while often passing on the task of exfiltrating data to others. Segmented tasking among various groups and sophisticated support infrastructure are among the tactics intelligence officials have revealed to Congress to show the hacking is centrally coordinated, the person said. US investigators estimate the ring is made up of anywhere from several dozen hackers to more than one hundred, said the person, who declined to be identified because the matter is secret.

(U) “The guys who get in first tend to be the best. If you can’t get in, the rest of the guys can’t do any work,” said the chief security officer for Mandiant Corp., an Alexandria, Virginia-based security firm that specializes in cyber espionage. “We’ve seen some real skill problems with the people who are getting the data out. I guess they figure if they haven’t been caught by that point, they’ll have as many chances as they need to remove the data.”

(U) Secretive Companies

(U) US companies have been secretive about the details of their computer security. When Google announced in 2010 that China-based hackers had raided its networks, it was a rare example of a US company publicly revealing a cyberburglary aimed at its intellectual property, in this case, its source code. Mountain View, California-based Google, the world’s largest search-engine firm, said at the time that at least 34 other major companies were victims of the same attack. However, only two, Intel and Adobe Systems Inc, stepped forward, and they provided few specifics.

(U) Google vastly underestimated the scope of the spying. Intelligence documents obtained by Bloomberg News show that China-based hackers have hunted technology and information across dozens of economic sectors and in some of the most obscure corners of the economy, beginning in 2001 and accelerating over the last three years. Many of the victims have been hacked more than once.

(U) One victim of the hacking ring, Associated Computer Systems, a division of Xerox Corp, provides back-office services such as accounting and human resources for thousands of multinational firms and government agencies in more than 100 countries. According to its website, ACS’s expertise includes digitizing and storing documents, a potential treasure-trove of information on the firm’s corporate clients, including carmakers and computer companies.

(U) Other targets of the group include large companies such as Hewlett-Packard, Volkswagen and Yahoo! Inc. Smaller firms in strategic sectors were also hit, such as iBahn and Innovative Solutions & Support Inc, which manufactures flight-information computers; as were Massachusetts Institute of Technology, the Italian Academic and Research Network and the California State University Network. An informal working group of private-sector cybersecurity experts and government investigators identified the victims by tracing information sent from hacked company networks to spy group-operated command-and-control servers, according to a person familiar with the process. In some cases, the targets aren’t aware they were hacked.

(U) ‘Operation Shady Rat’

(U) Details of a set of intrusions were originally published in an August, 2011 report by the cybersecurity firm dubbed “Operation Shady Rat.” The report didn’t name the country where the hackers were based or identify the private-sector victims. The report’s principal author, Dmitri Alperovitch, who now heads his own firm, Asymmetric Cyber Operations, confirmed the country was China.
In one of the earliest attacks on a company, cyberspies hacked into the computer networks of POSCO, the South Korean steel giant, in July 2006, Alperovitch said. The intrusion took place the same month that the steelmaker, the third largest in the world, initiated a takeover of a large steel mill in eastern China, according to the US-based Epoch Times, founded by supporters of the dissident Falun Gong spiritual sect, which first noted a link between the two events.

Two years later, Chinese rescue workers were using satellite communications equipment made by the Danish technology firm Thrane & Thrane, AS, following a major earthquake in Sichuan province. China Daily, the quasi-official newspaper, had praised the Danish equipment’s performance. Alperovitch said the Danish firm was hacked by the Shady Rat crew three months later. “With fans like those, who needs enemies?” he said. A spokesman for the Lundtofte, Denmark-based Thrane & Thrane, said although he couldn’t “rule out” that hackers breached their networks, no confidential data was taken. POSCO said hackers didn’t access critical networks or intellectual property.

The approval of China’s most recent five-year economic plan provides another possible link between Chinese government policy and cyber-espionage. The plan, approved by the National People’s Congress in March, identifies seven priority industries that mirror the most prominent targets of China-based cyberspies, according to the two senior US intelligence officials who have knowledge of the victims. KPMG International, the auditing firm, said the five-year plan’s priorities include clean energy; biotechnology; advanced semiconductors; information technology; high-end manufacturing, such as aerospace and telecom equipment; and biotechnology, including drugs and medical devices.

In many cases, the iBahn hackers appear to be working off the same shopping list, according to intelligence documents. In the biotechnology sector, their victims include Boston Scientific, the medical device maker, as well as Abbott Laboratories and Wyeth, the drug maker that is now part of Pfizer Inc. The hackers also rifled networks of the Parkland Computer Center in Rockville, Maryland, according to documents provided to Bloomberg News by a person involved in government tracking of the cyberspies, who declined to be identified because the matter isn’t public. Parkland is the computing center for the Food and Drug Administration, which has access to drug trial information, chemical formulas and other data for almost every important drug sold in the United States.

In the manufacturing sector, San Jose, California-based Cypress Semiconductor Corp, which makes advanced chips for telecommunications equipment, was a victim, as were Aerospace Corp, which provides scientific research on national security-related space programs, and Environmental Systems Research Institute, a Redlands, California-based company that develops mapping software. In China, those industries are developing rapidly. Chinese companies were involved in 10 of the 13 global technology initial public offerings in the third quarter of 2011, according to PricewaterhouseCoopers LLP, the global auditing firm. The Chinese firms specialized in information technology, semiconductors and clean energy, like solar power, the PwC report said.

Driving China’s spike in cyberspying is the reality that hacking is cheaper than product development, especially given China’s vast pool of hackers, said a fourth US intelligence official. That pool includes members of its militia, who hack on commission, the official said. They target computing, high
technology and pharmaceutical companies whose products take lots of time and money to develop, the official said.

(U) UN Security Council

China, a member of the UN Security Council, has the power to veto multilateral initiatives aimed at the country that pass through that body. Sanctions on Chinese goods in sectors that have been heavily targeted by cyberspies, green energy, semiconductors and pharmaceuticals, would be a problematic solution, probably sparking a trade war, said a cyber security expert at the Center for Strategic and International Studies in Washington. US government officials considering whether major corporate networks should be protected as a national security asset face opposition even from some victims protective of the Internet’s laissez-fair culture, said a senior fellow for counterterrorism and national security studies at the Council on Foreign Relations. “The situation we are in now is the consequence of three decades of hands-off approach by government in the development of the Internet,” he said.

(U) Lack the Leverage

(U) For now, administration officials have correctly assessed that they lack the leverage to compel China to change its alleged criminal behavior, he said. “The Cold War is a pretty good analogy,” the Council on Foreign Relations senior fellow noted. “There was never any serious effort to change the internal character of Soviet state.” At a minimum, the November intelligence agency report does throw down a marker in that conflict, said Estonian Defense Minister Mart Laar. Estonia, which suffered a massive cyber attack in 2007 it said originated from Russia, is pushing for a NATO cyber defense alliance. “I remember how the Cold War was changed, and you could for the first time feel the Soviet defeat coming when Ronald Reagan called the Evil Empire evil,” Laar said.

(U) CYBERSECURITY SPECIAL FOCUS FOR INDUSTRY:


(U) The first sign of trouble was a mysterious signal emanating from deep within the US military’s classified computer network. Like a human spy, a piece of covert software in the supposedly secure system was “beaconing”, trying to send coded messages back to its creator. An elite team working in a windowless room at the National Security Agency soon determined that a rogue program had infected a classified network, kept separate from the public Internet, which harbored some of the military’s most important secrets, including battle plans used by commanders in Afghanistan and Iraq.

(U) The government’s top cyberwarriors couldn’t immediately tell who created the program or why, although they would come to suspect the Russian intelligence service. Nor could they tell how long it had been there, but they soon deduced the ingeniously simple means of transmission, according to several current and former US officials. The malicious software, or malware, caught a ride on an everyday thumb drive that allowed it to enter the secret system and begin looking for documents to steal. Then it spread by copying itself onto other thumb drives.

(U) Pentagon officials consider the incident, discovered in October 2008, to be the most serious breach of the US military’s classified computer systems. The response, over the past three years, transformed the government’s approach to cybersecurity, galvanizing the creation of a new military command charged with bolstering the military’s computer defenses and preparing for eventual offensive operations. The efforts to neutralize the malware also demonstrated the importance of computer espionage in devising
effective responses to cyber threats. But the breach and its aftermath also have opened a rare window into the legal concerns and bureaucratic tensions that affect military operations in an arena where the United States faces increasingly sophisticated threats. Like the running debates over the use of drones and other evolving military technologies, rapid advances in computing capability are forcing complex deliberations over the appropriate use of new tools and weapons.

(U) This article, which contains previously undisclosed information on the extent of the infection, the nature of the response and the fractious policy debate it inspired, is based on interviews with two dozen current and former US officials and others with knowledge of the operation. Many of them assert that while the military has a growing technical capacity to operate in cyberspace, it lacks authority to defend civilian networks effectively. “The danger is not so much that cyber capabilities will be used without warning by some crazy general,” said a former NSA general counsel. “The real worry is they won’t be used at all because the generals don’t know what the rules are.”

(U) A furious investigation

(U) The malware that provoked the incident had circulated on the Internet for months without causing alarm, as just one threat among many. Then it showed up on the military computers of a NATO government in June 2008, according to the chief research officer of a Finnish firm that analyzed the intruder. He dubbed it “Agent.btz,” the next name in a sequence used at his company, F-Secure. “Agent.bty” was taken. Four months later, in October 2008, NSA analysts discovered the malware on the Secret Internet Protocol Router Network, which the Defense and State departments use to transmit classified material but not the nation’s most sensitive information. Agent.btz also infected the Joint Worldwide Intelligence Communication System, which carries top-secret information to US officials throughout the world.

(U) Such networks are typically “air-gapped”, physically separated from the free-for-all of the Internet, with its countless varieties of malicious code, such as viruses and worms, created to steal information or damage systems. Officials had long been concerned with the unauthorized removal of classified material from secure networks; now malware had gotten in and was attempting to communicate to the broader Internet. One likely scenario is that an American soldier, official or contractor in Afghanistan, where the largest number of infections occurred, went to an Internet cafe, used a thumb drive in an infected computer and then inserted the drive in a classified machine. “We knew fairly confidently that the mechanism had been somebody going to a kiosk and doing something they shouldn’t have as opposed to somebody who had been able to get inside the network,” one former official said. Once a computer became infected, any thumb drive used on the machine acquired a copy of Agent.btz, ready for propagation to other computers, like bees carrying pollen from flower to flower. But to steal content, the malware had to communicate with a master computer for instructions on what files to remove and how to transmit them.

(U) These signals, or beacons, were first spotted by a young analyst in the NSA’s Advanced Networks Operations (ANO) team, a group of mostly 20- and 30-something computing experts assembled in 2006 to hunt for suspicious activity on the government’s secure networks. Their office was a nondescript windowless room in Ops1, a boxy, low-rise building on the 660-acre campus of the NSA. ANO’s operators are among 30,000 civilian and military personnel at NSA, whose main mission is to collect foreign communications intelligence on enemies abroad. The agency is forbidden to gather intelligence on Americans or on US soil without special authorization from a court whose proceedings are largely secret.

(U) NSA, whose employees hold 800 PhDs in mathematics, science and engineering, is based at Fort Meade, an Army base between Baltimore and Washington that has the world’s largest collection of supercomputers as well as its own police force and silicon-chip plant. The ANO operators determined that
the breach was serious after a few days of furious investigation. On the afternoon of Friday, Oct. 24, the NSA’s top computer systems protection officer, was in an agency briefing with President George W. Bush, who was making his last visit to the NSA before leaving office. An aide handed the officer a note alerting him to the breach. At 4:30 pm, the officer entered the office of Gen. Keith Alexander, the NSA director and a veteran military intelligence officer. Alexander recalled that the officer minced no words. “We’ve got a problem,” he said.

(U) Permanent Slumber

(U) That evening, NSA officials briefed top levels of the US government: the chairman of the Joint Chiefs of Staff, the deputy defense secretary and senior congressional leaders, telling them about the incident. Working through the night, the ANO operators pursued a potential fix. Since Agent.btz was beaconing out in search of instructions, perhaps they could devise a way to order the malware to shut itself down. The next morning, in a room strewn with empty pizza boxes and soda cans, they sketched out their plan on a white board. But before it could be put into action, the NSA team had to make sure it would not affect the performance of other software, including the programs that battlefield commanders use for intelligence and communications. They needed to run a test. “Our objective,” recalled the computer systems protection officer, “was first, do no harm.”

(U) That afternoon, the team members loaded a computer server into a truck and drove it to a nearby office of the Defense Information Systems Agency, which operates the department’s long-haul telecommunications and satellite networks. At 2:30 p.m. they activated a program designed to recognize the beaoning of Agent.btz and respond. Soon after, the malware on the test server fell into permanent slumber. Devising the technical remedy was only the first step. Defeating the threat required neutralizing Agent.btz everywhere it had spread on government networks, a grueling process that involved isolating individual computers, taking them offline, cleaning them, and reformatting hard drives.

(U) A key player in the investigation was NSA’s Tailored Access Operations (TAO), a secretive unit dating to the early 1990s that specialized in intelligence operations overseas focused on gathering sensitive technical information. These specialists ventured outside the military’s networks to look for Agent.btz in a process called “exploitation” or electronic spying. The TAO identified new variants of the malware and helped network defenders prepare to neutralize them before they infected military computers. “It’s the ability to look outside our wire,” said one military official.

(U) Officials debated whether to use offensive tools to neutralize the malware on non-military networks, including those in other countries. The military’s offensive cyber unit, Joint Functional Component Command — Network Warfare, proposed some options for doing so. Senior officials rejected them on the grounds that Agent.btz appeared to be an act of espionage, not an outright attack, and didn’t justify such an aggressive response, according to those familiar with the conversations. As the NSA worked to neutralize Agent.btz on its government computers, the United States Strategic Command, which oversees deterrence strategy for nuclear weapons, space and cyberspace, raised the military’s information security threat level. A few weeks later, in November, an order went out banning the use of thumb drives across the Defense Department worldwide. It was the most controversial order of the operation.

(U) Agent.btz had spread widely among military computers around the world, especially in Iraq and Afghanistan, creating the potential for major losses of intelligence. Yet the ban generated backlash among officers in the field, many of whom relied on the drives to download combat imagery or share after-action reports. The NSA and the military investigated for months how the infection occurred. They retrieved thousands of thumb drives, many of which were infected. Much energy was spent trying to find “Patient Zero,” officials said. “It turned out to be too complicated,” said one. “We could never bring it down to as clear as: ‘that’s the thumb drive.’” The rate of new infections finally subsided in early 2009. Officials say
no evidence emerged that Agent.btz succeeded in communicating with a master computer or in putting secret documents in enemy hands. The ban on thumb drives has been partially lifted because other security measures have been put in place.

(U) ‘A great catalyst’

(U) The incident and investigation bolstered the argument for creating Cyber Command, a new unit designed to protect the military’s computer and communications systems. It gave NSA Director Alexander the platform to press the case, advocated by others, that the new command should be able to use the NSA’s capabilities to obtain foreign intelligence to defend the military’s systems. “It was a great catalyst,” said Alexander, although the effort later faced questions about whether the head of the largest and most secretive intelligence agency should also lead the new organization. The new organization, which has a staff of 750 and a budget of $155 million, brings together the Joint Task Force-Global Network Operations, which carried out the bulk of the cleanup work and the Network Warfare unit, the military’s offensive cyber arm. It began full operations on Oct. 31, 2010, with Alexander as its head.

(U) But the creation of Cyber Command did not resolve several key debates over the national response to cyberthreats. Agent.btz provoked renewed discussion among senior officials at the White House and key departments about how to best protect critical private-sector networks. Some officials argued that the military was better equipped than the Department of Homeland Security to respond to a major destructive attack on a power grid or other critical system, but others disagreed. “Cyber Command and [Strategic Command] were asking for way too much authority” by seeking permission to take “unilateral action inside the United States,” said Gen. James E. Cartwright Jr., who retired as vice chairman of the Joint Chiefs in August.

(U) Officials also debated how aggressive military commanders can be in defending their computer systems. “You have the right of self-defense, but you don’t know how far you can carry it and under what circumstances, and in what places,” Cartwright said. “So for a commander who’s out there in a very ambiguous world looking for guidance, if somebody attacks them, are they supposed to run? Can they respond?” Questions over the role of offense in cybersecurity deterrence began in the 1990s, if not earlier, said a Rand Corp. cyberwarfare expert. One reason it is so difficult to craft rules, he said, is the tendency to cast cyberwar as “good, old-fashioned war in yet another domain.” Unlike conventional and nuclear warfare, cyberattacks generally are enabled only by flaws in the target system, he said. Another reason it is so difficult, said a senior fellow at the Center for Strategic and International Studies, is the overlap between cybersecurity operations and the classified world of intelligence. “The link to espionage is where the nuclear precedent breaks down and makes cyber closer to covert operations,” he said.

(U) By the summer of 2009, Pentagon officials had begun work on a set of rules of engagement, part of a broader cyberdefense effort called Operation Gladiator Phoenix. They drafted an “execute order” under which the Strategic and Cyber commands could direct the operations and defense of military networks anywhere in the world. Initially, the directive applied to critical privately owned computer systems in the United States. Several conditions had to be met, according to a military official familiar with the draft order. The provocation had to be hostile and directed at the United States, its critical infrastructure or citizens. It had to present the imminent likelihood of death, serious injury or damage that threatened national or economic security. The response had to be coordinated with affected government agencies and combatant commanders. And it had to be limited to actions necessary to stop the attack, while minimizing impacts on non-military computers. “Say someone launched an attack on the United States from a known Chinese army computer, a known hostile computer,” the official said. “You could maybe disable the computer, but you’re not talking about making it explode and killing somebody.”
UNCLASSIFIED

(U) Turf battles

But the effort to create such comprehensive rules of engagement foundered, said current and former officials with direct knowledge of the policy debate. The Justice Department feared setting a legal precedent for military action in domestic networks. The CIA resisted letting the military infringe on its foreign turf. The State Department worried the military would accidentally disrupt a server in a friendly country without seeking consent, undermining future cooperation. The Department of Homeland Security, meanwhile, worked to keep its lead role in securing the nation against cyberthreats. The debate bogged down over how far the military could go to parry attacks, which can be routed from server to server, sometimes in multiple countries. “Could you go only to the first [server] you trace back to? Could you go all the way to the first point at which the attack emanated from? Those were the questions that were still being negotiated,” said a former US official. The questions were even more vexing when it came to potentially combating an attack launched from servers within the United States. The military has no authority to act in cyberspace when the networks are domestic, unless the operation is on its own systems.

(U) In October 2010, Pentagon officials signed an agreement with the Department of Homeland Security pledging to work to enhance the nation’s cybersecurity. But in speeches, Alexander, the head of Cyber Command, has suggested that more needs to be done. “Right now, my mission as commander of US Cyber Command is to defend the military networks,” he said in an April speech in Rhode Island. “I do not have the authority to look at what’s going on in other government sectors, nor what would happen in critical infrastructure. That right now falls to DHS. It also means that I can’t stop it, or at network speed see what’s happening to it. What we do believe, though, is that that needs to be accounted for. We have to have a way to protect our critical infrastructure.” Homeland Security Secretary Janet Napolitano, in a speech in California that same month, made her preference clear. “At DHS, we believe cyberspace is fundamentally a civilian space.” The executive order was signed in February. The standing rules of engagement limit the military to the defense of its own networks and do not allow it to go outside them without special permission from the president.

(U) The next vulnerability?

(U) Almost from the beginning, US officials suspected that Russia’s spy service created Agent.btz to steal military secrets. In late 2008, Russia issued a denunciation of the allegation, calling it “groundless” and “irresponsible.” Former officials say there is evidence of a Russian role in developing the malware, but some doubt whether the spy service created Agent.btz to infiltrate US military computers. Some say it could have been a product of Russia’s sophisticated mafia, with its extensive computer expertise, to collect all sorts of protected records worth stealing, or selling to the highest bidder. Or there could have been Russian involvement in one phase of the malware’s development before it was adapted by others. Others say they have no doubt that it was intentionally aimed at the Defense Department. New versions of Agent.btz continue to appear, years after it was discovered.

(U) What is clear is that Agent.btz revealed weaknesses in crucial US government computer networks, vulnerabilities based on the weakest link in the security chain: human beings. The development of new defenses did not prevent the transfer of massive amounts of information from one classified network to the anti-secrecy group WikiLeaks, an act that the government charges was carried out by an Army intelligence analyst. NSA analysts know how to neutralize Agent.btz and its variants, but no one knows when the next vulnerability will be discovered or what kind of intrusion might ensue. The individual, who was the NSA information assurance technical director until his retirement this year, said that in the early days of the investigation, a four-star general asked when the danger from Agent.btz would pass and heightened security measures could end. “We had to break the news to him,” the assurance technical director recalled, “that this is never going to be over.”

UNCLASSIFIED

25
(U) Top Ten Cybersecurity Stories of 2011 (www.nextgov.com, 30 DEC 11)

(U) The year 2011 proved to be a busy one on the cybersecurity front, with significant attention being paid to attacks, breaches and general security issues. Hackers' exploits this year were not necessarily new, but neither was the prioritization of the issue by policymakers, the media, and to a lesser extent, the private sector. Those who have been around the cybersecurity space for a while have seen much of this movie before -- though maybe this year was not a remake of the same film, but rather a sequel that just has some familiarity to it.

(U) So looking back on the year, what were the top stories? Here is a list, in no particular order, though several other high-profile hacks and government actions, could have easily made the list as well.

(U) • Fingers point to China as a cyber threat: This past year, we saw more attention being paid to China as a cybersecurity threat to both government and corporate systems. The theft of intellectual property and proprietary information from remote systems often had companies and the federal government wondering if the Asian nation was behind the breaches and attacks. In particular, McAfee's exposure of Operation Shady RAT (remote access tool), which revealed that more than 72 organizations, including multiple governments, the United Nations, corporations and various others had been compromised over a five year period. Experts were quick to point to China as being behind the operation.

(U) • Even Security Companies are at Risk: the EMC Corp.'s RSA Breach. In March, RSA warned that it had been a victim of a data breach and that its SecureID token authentication technology may have been compromised. The attack on one of the premiere "security" companies of the world, was a reminder that no one is safe from attack. It also had repercussions as companies rushed to replace their SecureID tokens, especially in critical industries such as banking and defense. Indeed, an attack on Lockheed Martin in May traced back to the RSA theft and it was largely believed that attacks on Northrop Grumman and L-3 Communications were also related to the RSA theft. In response to the attacks, RSA agreed to replace the tokens of many of its clients.

(U) • Duqu Trojan: One of Five Stuxnet's Cousins. September saw the introduction of the Duqu Trojan, which attacks Microsoft Window systems using a zero-day vulnerability. Many believed the virus was related to Stuxnet, the worm discovered in 2010 that was said to be a threat to SCADA systems in Iran. Just yesterday, researchers revealed that Duqu and Stuxnet may be members of a larger family -- they've discovered commonalities between the two malware and at least three other malware. If that is the case, then this will be one of the top stories of 2012 as experts search for the identity of whoever (or whatever nation) created the malware.

(U) • Hacktivists: LulzSec and Anonymous. While Anonymous might be better termed a movement than a hacking gang, its collective activities in 2011 drew a significant amount of attention. Among its victims were HB Gary Federal, Sony (more than once), the Westboro Baptist Church, Bank of America, Stratfor, the Los Zetas drug cartel and various government entities. Another group that was active was LulzSec, which also attacked Sony, as well as PBS, Fox News, Nintendo, Bethesda Game Studios, and various governments and banks. In June, both hacktivist groups teamed up for "Operation Anti-Security," which they claimed was intended to protest government censorship and monitoring of the Internet.

(U) • News of the World: Hacking Gone Wild: Hacking, or in this case, phone phreaking, went mainstream when it was revealed in July that News Corporation's News of the World hired an investigator to hack into a missing teenager's phone and delete messages. The news became more scandalous when it was revealed that they not only hacked into the murdered teen's phone, but possibly...
into the phones of families of British servicemen killed in action. Following the revelation, the paper folded and many of its former editors were arrested and/or jailed.

(U) • Epsilon: Data Breach Makes it Personal for Customers. In April, online marketer Epsilon revealed that it had been a subject of, yes, you guessed it, a hack. The names and emails of potentially millions of individuals were compromised. According to experts who analyzed the situation, the customers of the following companies may have had their information stolen: Kroger, TiVo, US Bank, JPMorgan Chase, Capital One, Citi, Home Shopping Network, Ameriprise Financial, LL Bean Visa Card, McKinsey & Company, Ritz-Carlton Rewards, Marriott Rewards, New York & Company, Brookstone, Walgreens, The College Board, Disney Destinations, Best Buy and Robert Half Technologies. Soon after the attack, these companies, along with numerous other Epsilon customers, began sending emails to their customers warning that their information may have been compromised and to be aware of email spam and phishing attacks.

(U) • Mobile and Vulnerable; When your Phone is Not Your Friend: As more people flocked to smartphones in 2011, so did the hackers and the privacy activists. On the hacking side, revelations that malware was spreading rapidly on smartphones, especially as the Android Market and similar sites allowed users to load apps that had not been checked for security. At the same time, apps that seem like one thing but actually come associated with fees, continue to proliferate on mobile devices. On the privacy side, the Carrier IQ scandal, along with concerns over geolocation privacy, made people more aware of just how much their phones know (and share) about them.

(U) • Congress; Cybersecurity Legislation, Here We Come!: Congress continued to say that cybersecurity was a priority this year. In the House, the newly elected Republican Leadership created a Task Force, under the leadership of Rep. Mac Thornberry, R-Texas, to put together recommendations on cybersecurity legislation. The group's report came out in the second half of the year, with two bills following its release -- an information sharing bill in the House Intelligence Committee and an information sharing bill in the House Homeland Security Committee. Other Committees, including the Judiciary Committee, are expected to move legislation in the new year. Senate Leader Harry Reid, D-Nev., introduced a "shell" bill outlining priorities and tasking several Senate Chairs, including Homeland Security and Government Affairs Chairman Sen. Joe Lieberman, I-Conn., Commerce's Sen. Jay Rockefeller, D-W.V., Intelligence's Sen. Dianne Feinstein, D-Calif., Armed Service's Carl Levin, D-Mich., and Judiciary's Sen. Patrick Leahy, D-Vermont, to put together a comprehensive bill. Sections of a potential bill have been circulating and the Majority Leader has indicated that a bill will come to the Senate floor in the new year.

(U) • Nasdaq: Should Investors Worry?: In February, the Nasdaq Stock Exchange discovered suspicious files on its servers, apparently put on the system by hackers. There was much concern that Nasdaq was not the true target but that an intruder was targeting executives at companies who use part of the Nasdaq server that was attacked. Perhaps Nasdaq was only the vehicle by which hackers could reach top corporations? If that was the case, the incident certainly puts a new twist on the meaning of a Trojan horse.

(U) • Operation Ghost Click: And Now, to End on a Positive Note . . . In November, six Estonian nationals were arrested for running one of the most significant Internet fraud rings that law enforcement has cracked. The ring used malware to infect approximately 4 million computers in more than 100 countries. The infected computers were being used to make at least $14 million in Internet advertising
(U) CYBER THREAT ITEMS FROM THE PRESS

(U) Aggressive Phishing Attack Targets Military Personnel (Information Week, 28 DEC 2011)

(U) Emails containing malware, which appear to come from senior officers or legit companies, have been sent to military personnel during the holiday season. The US military received an unwanted present this Christmas holiday season in the form of an "aggressive" phishing attack that's been making the rounds of .mil email accounts, according to the Army. There are several attacks making the rounds, the most notable coming in the form of an email with the subject line "Deposit Posted" that appears to be from USAA, a financial services company that services members of the military as well as their families and veterans, according to an article on the US Army's website. The email asks people to open a file infected by Zeus malware that can access people's personal information and even require a complete reinstall of a computer's operating system.

(U) Other attacks have targeted US military installations and defense facilities with emails that appear to come from senior officers or military authority figures. Those emails also request that the recipient download and install software that's depicted as a "critical security measure that must be immediately deployed," according to the Army. But rather than providing security, the software instead is either a Trojan Horse that can destroy systems and networks or data-mining software that can provide hackers with unauthorized access to information behind the firewall.

Phishing is usually an unsolicited email that appears to be coming from a legitimate institution, such as a bank or other financial company, that asks a recipient to give up personal information or download software. The military is asking its members to be cautious when opening any unsolicited email requests to download software or access secure information. Phishing has consistently been one of the biggest security threats to the US government for a number of years, although the number of actual incidents have been slacking off while other types of attacks have been on the rise, according to the United States Computer Emergency Readiness Team (US-CERT), which keeps track of US cybersecurity incidents.

(U) Still, the feds should remain wary of these types of attacks, which can wreak havoc if people fall for them. The Department of Energy's Oak Ridge National Laboratory shut down email and Internet access for more than a week in April after a sophisticated phishing attack that was sent to about 570 email accounts.

(U) Security Trumps Secrecy in Cyber Fight, Prosecutor Says (Reuters, 12 JAN 2012)

(U) A top federal prosecutor has a message for companies: If you've been hacked, tell us. Speaking at a cyber security conference in New York in January, Manhattan US Attorney Preet Bharara said companies should trust in the discretion of prosecutors and the FBI and come forward with information about a security breach, rather than keep it an internal secret. "When industry delays or minimizes, it is harder to assess vulnerabilities and harder to formulate solutions," Bharara said. "When industry delays unduly in disclosing to us, or minimizes, it is that much harder to get the bad guy."

(U) Cyber security experts say that corporations rarely acknowledge breaches, and often keep them secret from law enforcement out of fear that news of a compromise will damage their reputation, hurt stock prices and possibly lead to further attacks. Bharara addressed that fear, calling it unacceptable in the face of increasingly virulent cyber attacks. Trying to maintain secrecy was "the equivalent of sticking one's head in the sand," Bharara said. "Get over it."
In January 2010, Google Inc acknowledged that it had been the victim of a cyber attack, reporting that it was one of at least a score of major corporations that had been targeted by hackers in China. Security experts have since said that they notified dozens of other companies that they were also victimized by the same hackers, but only a handful have acknowledged that they were involved in what has become known as the Aurora attacks. Once cases come to court, however, federal prosecutors in Manhattan have on some occasions gone to great lengths to help preserve company secrets. When a now-jailed former programmer at Goldman Sachs was tried in Manhattan federal court on charges he stole computer code for the investment bank's high-frequency trading platform, prosecutors asked the judge to seal certain proceedings to preserve the secrecy of Goldman's system from competitors.

Analyst Comment: Companies in Florida that experience breaches or hacking attempts should immediately contact the FBI Tampa Cyber squad. As this article points out, confidentiality of corporate data is very important.

Anonymous Targets New York Officials and Companies (International Business Times, 05 JAN 2012)

Anonymous, the leaderless hacktivist collective, has targeted New York's top officials, companies and organizations as part of one of its latest operations. Dubbed Operation Hiroshima, or #OpHiroshima, the New Year's Day document dump was an attempt to "dox," or release revealing information, about a wide range of targets through a variety of internet channels. New York's top politicians were not spared the Anonymous treatment, as documents containing personal, financial and professional information were released on Mayor Michael Bloomberg, Governor Andrew Cuomo, NYPD Commissioner and NYPD Executive Director Kevbin Holloran as part of the operation. The New York Stock Exchange and Time Warner CEO Jeffrey Bewkes were also targeted under the #OpHiroshima document dump, as were members of the US Senate who voted for the National Defense Authorization Act (aka: NDAA), including New York's Chuck Schumer and Kirsten Gilligrand.

But New York was not the only area targeted under the widespread doxing operation. The Boston and Oakland police departments were also hit with doc dumps, as were UC Davis, and a range of Washington officials including federal judge Liam O'Grady and FBI Director Robert Mueller. The document dump exposed key information such as the targets' personal addresses, e-mails and phone numbers, family members and financial statements. It is difficult to determine whether or not the documents are classified, and whether they were obtained from people who have access to such files through their employers, through the work of hackers, or through legitimate means of accessing governmental records, such as Freedom of Information Act requests.

There has been very little coverage in mainstream media of the #OpHiroshima leaks, which also released a wide range of government documents on topics as varied as the war in Afghanistan and global governance. A YouTube video released by Anonymous on Dec. 24 featured a montage of news footage before switching to a robotic voice which explains the purpose of Operation Hiroshima while an Anonymous symbol occupies the screen. "On Jan. 1, 2012, at 12 a.m., every last piece of information on you corrupt individuals we have acquired through our individual skills will be released all across the Web everywhere," the narrator states. "What is the point of this? Well, it's to show that we still run this. You take our speech, you take our Internet, you take our Bill of Rights, you take our Constitution, we fight back. Get ready for a new year: 2012, a year of Anonymous. Operation Hiroshima engaged."
‘Anonymous’ Back With A Vengeance: Downs DoJ, MPAA, RIAA, Universal Music Websites; White House also Targeted as Federal Anti-Piracy Moves Fuel Widespread Online Attacks (Dark Reading, 19 JAN 2012)

In apparent retaliation for the federal takedown of online storage and file transfer site Megaupload announced by the Department of Justice today, the Anonymous hacktivist collective went to work waging mass distributed denial-of-service (DDoS) attacks against websites of the DoJ, Motion Picture Association of America, the Recording Industry Association of America, and Universal Music that knocked those sites offline.

Also in the crosshairs of the hacktivists: the White House website, which as of this posting remained online, although Anonymous members were calling for targeting it as well. And security experts say this latest, and possibly biggest, DDoS campaign by Anonymous is far from over, with more targets to come. According to one tweet from AnonDaily, this is the largest attack by the hacktivist group, with more than 5,600 people using the Low Orbit Ion Cannon (LOIC) DDoS tool. A former member of Anonymous who is now an online activists entity called Project PM, tweeted about another Anonymous campaign focused on Democratic members of Congress who remain in support anti-piracy bills before Congress, the House’s Stop Online Piracy Act (SOPA), and the Senate’s Protect Intellectual Property Act (PIPA).

The wave of DDoS attacks in January came in reaction to DoJ’s announcement today that it had issued 20 search warrants in nine countries, including the United States, and had seized $50 million in assets from Megaupload. Seven people were copyright infringement and operation of a global criminal organization, including site founder Kim Dotcom (aka Kim Schmitz), who was arrested in New Zealand with three other suspects. The individuals are accused of supporting illegal downloads of music, movies, and other copyrighted content. An unsealed grand jury indictment said Megaupload made $175 million in subscriptions and advertising, and cost copyright owners some $500 million in lost revenues. While the company was based in Hong Kong, US officials were able to take action because the company allegedly hosted some pirated content on servers in Ashburn, Virginia.

The timing couldn’t be more striking: the case hit the news one day after a high-profile online protest of SOPA and PIPA. Federal officials, however, told The Washington Post that it the timing of the indictment announcement was a coincidence. Megaupload posted a statement on its site prior to its takedown, stating that the allegations were “grotesquely overblown,” according to the AP. "The fact is that the vast majority of Mega’s Internet traffic is legitimate, and we are here to stay. If the content industry would like to take advantage of our popularity, we are happy to enter into a dialogue. We have some good ideas. Please get in touch," the statement said.

Meanwhile, Anonymous’ "OpMegaUpload" campaign is far from over, industry experts say. Look for other victims to face DDoS firepower as well. Yesterday’s online protest fervor coupled with today’s indictment merely fanned the flames for Anonymous and attracted more participants, one source said. Among the tweets from accounts claiming to be from Anonymous was one that said: "Megaupload was taken down w/out SOPA being law. Now imagine what will happen if it passes. The Internet as we know it will end. FIGHT BACK."
(U) US Shuts Megaupload.com, Hackers Retaliate *(Reuters, 20 JAN 2012)*

(U) The US government shut down the Megaupload.com content sharing website, charging its founders and several employees with massive copyright infringement, the latest skirmish in a high-profile battle against piracy of movies and music. The Department of Justice announced the indictment and arrests of four company executives in New Zealand in January as debate over online piracy reaches fever pitch in Washington where lawmakers are trying to craft tougher legislation. The movie and music industries want Congress to crack down on Internet piracy and content theft, but major Internet companies like Google and Facebook have complained that current drafts of the legislation would lead to censorship. A Justice Department official said the timing of the arrests was not related to the battle in Congress.

(U) New Zealand police raided a mansion in Auckland and arrested Megaupload founder Kim Dotcom, also known as Kim Schmitz, 37, a German national with New Zealand residency. About 70 police, some armed, raided 10 properties and also arrested the website's chief marketing officer, Finn Batato, 38, chief technical officer and co-founder Mathias Ortmann, 40, both also from Germany, and Dutch national Bram van der Kolk, 29, who is also a New Zealand resident. New Zealand police seized millions of dollars worth of assets, which included luxury cars such as a Rolls Royce Phantom Drophead Coupe, from the group, dubbed the "Mega Conspiracy" by prosecutors. They also seized more than NZ$10 million ($8 million) from financial institutions.

(U) "The FBI contacted New Zealand Police in early 2011 with a request to assist with their investigation into the Mega Conspiracy," said Detective Inspector Grant Wormald from the Organised & Financial Crime Agency New Zealand. "All the accused have been indicted in the United States. We will continue to work with the US authorities to assist with the extradition proceedings," Wormald said in a statement. The men appeared briefly in an Auckland court and were remanded in custody until Monday for a bail hearing. "We have nothing to hide," Kim Dotcom said from the dock after his lawyer opposed media cameras in the court, reported New Zealand media.

(U) Hackers Retaliate

(U) Vocal critics of the US Stop Online Piracy Act, or SOPA, and Protect IP Act (PIPA), quickly showed their opposition to the shutdown of Megaupload.com, with hackers attacking the public websites of the Justice Department, the world's largest music company Universal Music, and the two big trade groups that represent the music and film industries. "The government takes down Megaupload? 15 minutes later Anonymous takes down government & record label sites," a member of Anonymous said via Twitter. Representatives with the Justice Department and Recording Industry Association of America declined comment on the attacks. Officials with Universal Music could not immediately be reached. A Motion Picture Association of America spokesman said his group was working with law enforcement to identify the attackers.

(U) The Mega Conspiracy group was accused of engaging in a scheme that took more than $500 million away from copyright holders and generated over $175 million in proceeds from subscriptions and advertising, according to the indictment unsealed in January. "In exchange for payment, the Mega Conspiracy provides fast reproduction and distribution of infringing copies of copyrighted works from its servers located around the world," the indictment said. US Justice Department officials said that the estimate of $500 million in economic harm to copyright holders was on the low end and likely significantly more. The allegations included copyright infringement as well as conspiracy to commit copyright infringement, conspiracy to commit money laundering and conspiracy to commit racketeering.
(U) Racketeering, Money Laundering

(U) If convicted, the maximum penalties are 20 years for conspiracy to commit racketeering and to commit money laundering and five years for each count of copyright infringement and five years for conspiracy to commit copyright infringement. The companies charged, Megaupload Ltd and Vestor Ltd, were both registered in Hong Kong and owned either in large part or solely by Dotcom. A lawyer who has previously worked with Megaupload was not immediately available for comment.

(U) Megaupload has boasted of having more than 150 million registered users and 50 million daily visitors, according to the indictment. At one point, it was estimated to be the 13th most frequently visited website on the Internet. Users could upload material to the company's sites which then would create a link that could be distributed. The sites, which included video, music and pornography, did not provide search capabilities but rather relied on others to publish the links, the indictment said. Users could purchase memberships to the site to obtain faster upload and download services, the primary source of revenue. Material that was not regularly downloaded was deleted and financial incentives were offered for popular content, according to the charges. The web page with the link to the copyrighted material would include advertisements, another source of revenue. If copyright holders complained about a specific link to the website, prosecutors said that Megaupload.com would remove that link but scores of others existed to the same material, according to prosecutors. Other material found uploaded included child pornography and terrorism propaganda videos, according to the indictment. The US government's investigation began in March 2010.

(U) Cybercrime is a Growing Threat for Government and Public Sector Organizations (PC Advisor, 13 JAN 2012)

(U) Cybercrime is a growing threat for government and public sector organizations, after 14 percent admitted they have been the victim of a web-based scam. According to research by Pricewaterhouse Coppers, more than a quarter (28 percent) believe they are likely to suffer a cybercrime attack in the next 12 months while 40 percent admit they think the risk of cybercrime to be on the rise. "Damage to an organization's reputation and the potential loss of data are high on the public sector's agenda when it comes to the impact of cyber attacks," said PwC's head of information security in government. "This is hardly surprising given recent high profile cases of data security breaches. Therefore, it is vital that organizations continue to ensure they are investing in cybercrime monitoring capabilities and align their management structures to take timely actions if a cyber incident occurs."

(U) PwC added that while over half of public sector organizations claim to have in-house capabilities to detect cybercrime, most don't have the resources to investigate it and are reliant on external forensic technology investigators. "The statistics also indicate that the most senior people within organizations are not placing enough emphasis on the importance of managing the real threats that cybercrime frauds present to their organization, with nearly half of Boards not reviewing the threat more frequently than annually," added PwC’s head information security in government. Recently, PwC estimated the UK spent £3bn on cyber security last year. The total global spend on cyber security was $60bn and this figure is expected to grow by 10 percent year on year for the next three years.
(U) Viruses Stole City College of San Francisco Data for Years (The San Francisco Chronicle, 13 JAN 2012)

(U) Personal banking information and other data from perhaps tens of thousands of students, faculty and administrators at City College of San Francisco have been stolen in what is being called "an infestation" of computer viruses with origins in criminal networks in Russia, China and other countries, The Chronicle has learned. At work for more than a decade, the viruses were detected a few days after Thanksgiving, when the college's data security monitoring service detected an unusual pattern of computer traffic, flagging trouble.

It appeared at first that the problem was contained in a single computer lab at Cloud Hall on the Phelan Avenue campus, one of a dozen City College sites around the city. the College’s chief technology officer, immediately shut the lab down and reported the problem to the Chancellor, General Counsel and the President of the Board of Trustees. But a closer look revealed a far more nefarious situation, which had been lurking within the college's electronic systems since 1999. For now, it's still going on. So far, no cases of identity theft have been linked to the breach. That may change as the investigation continues, and college officials said they might need to bring in the FBI. The college's payroll, admissions and accounting systems have yet to be analyzed for the viruses. "We have to move as quickly as possible," the Chancellor said. "We don't know yet, but it doesn't mean there hasn't been a serious infection there, as well."

(U) They Troll at Night

(U) Each night at about 10 p.m., at least seven viruses begin trolling the college networks and transmitting data to sites in Russia, China and at least eight other countries, including Iran and the United States, the college’s CTO and his team discovered. Servers and desktops have been infected across the college district's administrative, instructional and wireless networks. It's likely that personal computers belonging to anyone who used a flash drive during the past decade to carry information home were also affected. Some of the stolen data is probably innocuous, such as lesson plans. But an analysis shows that students and faculty have used college computers to do their banking, and the viruses have grabbed the information, the CTO said.

(U) Although the extent of what has been transmitted is not yet clear, the CTO said the server with medical information for students and employees appears to be virus-free. "We may never know the full extent of the damage, and how many lives have been affected by this," the CTO told three college trustees who met in January to discuss school buildings and technology issues. "These viruses are shining a light on years of (security) neglect." State law requires that cyber victims be notified when personal information has been stolen, and college officials are trying to determine who needs to be told. The college is analyzing 17 computer systems thought to be at risk.

(U) Russian addresses

(U) Since Nov. 28, college officials have traced at least 723 Internet protocol addresses to the Russian Business Network, "a notorious gang in the business of stealing and selling personal information," the CTO said. Once known as "the granddaddy of online hosting networks for criminals," the Russian Business Network disbanded around 2008, according to computer security company Symantec of Mountain View. But criminals are still collecting the data, and American college students are often prime victims.
"Unfortunately, penetration into higher education is not uncommon," said a member of Symantec's data loss prevention team. "A lot of criminals see students as investments in the future - people with clean credit records who, if they get a college degree, will be high income and a good identity to steal." He said the criminals often hold onto the information for years as it becomes more valuable. Nearly 1 in 5 cyber security breaches are connected to higher education, he said.

Little protection

Places like City College of San Francisco, where officials have done little to protect against cyber attacks over the years, are especially vulnerable, the college CTO said. He arrived at City College in July 2010, and was astonished to learn how porous its computer systems have been. "When I found out they hadn't changed passwords in over 10 years, I hit the roof," said the tech expert, who ordered them all changed last summer. But cash-strapped City College has worse vulnerabilities than that, he said. They include poor network design and old equipment, a "draconian system" for agreeing on new policies - including urgent security issues - and little money for new, virus-resistant technology.

Some college leaders also suffer bouts of technophobia, he said, leading to lax attention to the need for cyber security. Hotchkiss' efforts to secure City College's computer systems have also run up against a competing need: academic freedom. Shortly before Hotchkiss arrived at City College, a new firewall was installed. Technicians set it up to block pornography sites, which are notorious for transmitting computer viruses. Then faculty began complaining to Hotchkiss that students needed access to porn sites. For research. Eventually, given examples of the academic necessity, Hotchkiss had to remove the porn block.

He eventually hired a data security service which detected the virus problem. On a January evening, three trustees listened to the collect CTO and the data security service network security chief scientist describe how they may be looking at only the tip of the problem. They talked about hundreds of thousands of dollars spent over the last 10 years on consultants who failed to secure the systems and learned that they lack even basic virus protections. "Given the outright mismanagement of our networks, if someone's information is stolen, are we liable for that?" a trustee asked. No one had an answer.

Analyst Comment: As this article points out, one hacker using an advanced persistent threat vector, such as a sophisticated spearphishing attack, gain access to a network, data will be exfiltrated to a remote network, often at night. Network administrators and IT security personnel should check network logs for this nighttime or weekend "beaconing", as it is an indicator of an APT attack. The FBI Tampa Cyber squad should also be contacted, as the can determine if the remote beaconing IP address is from a bad actor.

Major global businesses are calling for better intelligence- and information-sharing among themselves and other organizations hit by cyberattacks in order to better fend off the bad guys and protect themselves from breaches, but a universal model for doing so remains elusive. The goal of sharing attack information and intelligence among victim organizations and other organizations that also could become targets was part of a new set of recommendations issued today by security executives from major global firms including ABN Amro, ADP, BP, Coca-Cola, eBay, Genzyme, HSBC Holdings, Johnson & Johnson, JPMorgan Chase, Nokia, Northrop Grumman, SAP, T-Mobile, and RSA parent company EMC.
Their recommendations were included in a report published under the auspices of the Security for Business Innovation Council (SBIC) and facilitated by RSA.

(U) But getting business rivals as well as federal agencies and the private industry to join hands and share their attack experiences, logs, and artifacts is not so simple. Aside from competitiveness, privacy, and technical issues, there are legal ramifications that typically limit or altogether prevent businesses from helping one another. Even so, experts say it’s time for organizations to come out of the shadows and team up against the common enemy of cybercrime and cyberespionage. That’s the only way to get a leg up on the bad guys, they say.

(U) But so far the sharing has been either industry-specific or very much ad-hoc: The Defense Security Information Exchange is an online portal for Defense contractors to swap attack information, and some local organizations, such as the Bay Area CSO Council, which includes chief security officers from Adobe, eBay, Gap, eTrade, Symantec, SAIC, Lawrence Livermore Laboratory, PayPal, Cisco-WebEx, Yahoo, and Intel, confidentially share their attack information. There’s also InfraGuard, the FBI-led association of local businesses, academic institutions, and state and local law enforcement agencies that meet regionally to share attack and threat information.

(U) Lately, there have been more signs of cooperation: Key financial institutions, including Morgan Stanley and Goldman Sachs, in January took some of the first steps toward possibly establishing a central site to gather and analyze attack trends for the financial services industry. They met with researchers at the Polytechnic Institute of New York University to noodle about the possibility of such a center, while the Bank of America has also been holding informal meetings with banks on coming up with solutions to deter the latest threats. Meanwhile, Congress is currently floating multiple pieces of legislation that call for information-sharing with and among the feds, including a bill that would set up a national information-sharing organization as a way to protect critical infrastructure. But there’s still no official go-to place for sharing this type of information, and experts say it’s unclear if there ever will be.

(U) The executive chairman of RSA Security, says a hierarchical model for victim organizations to share their threat information isn’t likely to emerge. “It’s never going to be a top-down thing,” he says. “I foresee a future where there are networks of networks, until from the grassroots up we develop more of an online information-sharing facility, this whole idea of a neighborhood watched, expanded on a worldwide basis,” he says. Both the legal and overall scope of such a model have thus far been some of the biggest hurdles. It’s the smaller, more focused models like that of the Bay Area CSO Council that have found success. “The [Bay Area CSO] Council worked because it was formed with a prerequisite trust in the network. It was small enough, and the value and benefit was very clear,” says the former executive director of the Bay Area CSO Council and founder of the Union of Concerned Cybersecurity Leaders.

(U) The SBIC report says information-sharing among organizations requires the investment of manpower and technologies. “If something happens at your organization, the first question you’ll ask is, ‘Is it just me or is everybody else getting hit with this attack?’” said the chief information security officer for The Coca-Cola Company, a member of the SBIC in a statement. “You can’t answer that for yourself. And it takes too long to call 20 of your closest friends. You’ve got to be part of a larger gene pool to get an immediate answer to that question.” And other companies need to be willing to do the same, SBIC members say. "As cyber attacks continue to threaten enterprises and governments, more organizations will likely be motivated to invest in information sharing. An important factor paving the way is that organizations have the people, processes, and technologies in place to effectively participate in intelligence exchange," the report says.
RSA’s executive chairman says he has previously tried to pull together service providers, telcos, and security organizations to see how to construct such an entity. "We can’t get past the lawyers," he says. It’s the legal downsides that overshadow some of the possible benefits of getting an inside track on a new targeted attack campaign out of China, or a look at the latest malware variant going after corporate user accounts. "At the end of the day, there are a lot of legal downsides and not a lot of perceived upsides," the Union of Concerned Cybersecurity Leaders’ founder says. CSOs get frustrated when they share attack intelligence with the FBI, for example, and never hear back. Or they only get intelligence that’s expired or they can’t take action on, he says.

And in many cases, when the general counsel is brought in, it’s game over for any information-sharing about a breach. Even if new legislation legalizes the liability issues that block this sharing, there’s no guarantee organizations will suddenly clamor to spill their guts about breaches. RSA’s executive chairman says the current ad-hoc groups may just eventually coalesce into something bigger. "I am really encouraged by ... the ISACS and industry groups taking it on themselves," he says. They could eventually start connecting among one another, he says, and expand into a network of networks from there, for example.

But once you get the green light to share your breach data with others, then what? "Sharing information is not the end state. The end state is to get actionable information that will help improve corporations’ and governments’ cyber-security posture and continually raise the bar," the president and CEO for the Center for Internet Security, chair of the Multi-State Information Sharing and Analysis Center, and chair of the National Council of ISACs, in a statement.

At the heart of the SBIC’s recommendations is what it calls an "intelligence-driven information security" approach, where businesses gather reliable security information from government, industry, and internal sources to get a full picture of the threat and their exposures to it, and a process for analyzing it and taking action. "An intelligence-driven approach to information security can deliver comprehensive situational awareness, enabling organizations to more effectively detect and mitigate cyber attacks. Developing a cyber-risk intelligence capability will take investments in people, process, and technology. It will challenge the information-security team to grow beyond the current skill set and to commit to a change in mind-set. And it will require not only the steadfast efforts of the security team but also broad organizational support," the SBIC report says.

**Analyst Comment:** Florida private and public sector organizations and agencies are encouraged to join the Tampa FBI InfraGard chapter to receive up-to-date information on sector-specific threats and vulnerabilities.

**Banks Unite To Battle Online Theft** *(The Wall Street Journal, 10 JAN 2012)*

Rising cybersecurity threats are pushing big banks to do something that doesn't come naturally for these secrecy steeped institutions: share information with one another. In January security officials from Wall Street financial firms, including Morgan Stanley and Goldman Sachs Group Inc., were expected to meet with researchers from the Polytechnic Institute of New York University to discuss the creation of a new type of center that would sift through mountains of bank data to detect potential attacks, people familiar with the situation said. At the same time, Bank of America Corp. has begun hosting experts from other major banks at quarterly informal roundtables, in which the rivals try to devise solutions to cybersecurity threats, according to other people.
(U) Both initiatives are designed to encourage banks to work together to better protect against hackers, whose efforts to shut down electronic operations and steal money or customer data pose a growing concern for the industry. Sony Corp., the Central Intelligence Agency and Citigroup Inc. are just a few of the firms that cyber-rogues have targeted over the past year. Online attacks have increased sharply over the past two years and financial institutions are among the most likely targets, according to a new survey by PricewaterhouseCoopers LLP, the consulting firm. An analyst with Gartner Research expects financial companies to increase spending on fraud detection and customer authentication systems by as much as 12 percent to a record $1 billion, over the next two years.

(U) While many bank officials agree with the information-sharing in principle, some are concerned that doing so could provide rivals with too much insight into their operations. At the NYU-Poly meeting, for instance, some bank officials are expected to make the case that banks should scour their own data internally, rather than provide information to outside researchers, people familiar with the matter said. "The mentality of the banks has been, 'Let's do everything internally because we don't want to give anything away,' " said a managing partner with Chartis Research in London.

(U) But hackers are forcing banks to abandon that old go-it-alone mindset in favor of a more-inclusive approach, executives said. We realized that just as the fraudsters collaborate with each other, we as an industry must collaborate," said a Bank of America senior vice president of security. A graphic example of just how vulnerable banks are to hackers occurred in 2010, when security experts from major financial firms gathered in San Francisco for a conference. As panel after panel discussed cyber threats and how to guard against them, hackers carried out a real-life attack. Using what has come to be known as the Zeus Trojan, a type of software that infects computers and covertly tracks keystrokes to steal personal data, thieves penetrated bank computer firewalls and stole millions of dollars from their customers. The security experts attending the conference emailed each other furiously on their BlackBerrys and agreed to meet in person to discuss the threat, according to a person who was there. "That was the first time I remember people feeling open to talking about these threats," this person said.

(U) At the most-recent meeting hosted by Bank of America in late summer at its New York offices, executives discussed a type of online espionage that involves a long-term pattern of persistent hacking attempts known as "advanced persistent threats." That approach figured in recent hacks against RSA, a unit of EMC Corp., and Sony and are considered by most professionals to be the leading cybersecurity threat of the day.

(U) Banks also are working with Internet service providers in new ways to better authenticate email traffic to prevent hackers from impersonating employees and gaining access to customer data. Rather than forcing the ISPs to make an educated guess about which emails to let through, banks have started providing them with data that helps them better verify the messages, according to the company eCert Inc., a clearing house for such data.

(U) Sharing might be discouraged in other parts of banking, because of possible antitrust implications. But the practice has been mandated in the world of cybersecurity since 1998, when President Bill Clinton issued an order requiring the public and private sectors work together to protect critical infrastructure such as the financial system. In response to that order, financial firms created an industry group called the Financial Services Information Sharing and Analysis Center to encourage banks to work together.

(U) Still, it is only recently that banks have begun to lift the veil. At an industry conference in 2003, said the founder of IronKey, a security firm based in Sunnyvale, Calif., the chief technology officer of a large bank said "phishing" attacks used by cyber criminals to extract personal information were not a threat.
"I went up to him afterward and said, 'If they are not a threat, why are you spending $2 million on software to protect against them?'' he recalled. The executive's answer: 'We don't want to talk about fraud in front of anyone.'

(U) Malware Targets Bank Accounts; ‘Gameover’ Delivered Via Phishing E-Mails (www.fbi.gov; 06 JAN 2012)

(U) Cyber criminals have found yet another way to steal your hard-earned money: a recent phishing scheme involves spam e-mails, purportedly from the National Automated Clearing House Association (NACHA), the Federal Reserve Bank, or the Federal Deposit Insurance Corporation (FDIC), that can infect recipients’ computers with malware and allow access to their bank accounts. The malware is appropriately called “Gameover” because once it’s on your computer, it can steal usernames and passwords and defeat common methods of user authentication employed by financial institutions. And once the crooks get into your bank account, it’s definitely “game over.” Gameover is a newer variant of the Zeus malware, which was created several years ago and specifically targeted banking information.

(U) How Can You Protect Yourself?

- (U) - Obviously, make sure your computer’s anti-virus software is up to date

- (U) - Don’t click on e-mail attachments from unsolicited senders. NACHA, FDIC, and the Federal Reserve all say they don’t send out unsolicited e-mails to bank account holders. If you want to confirm there’s a problem with your account or one of your recent transactions, contact your financial institution directly

- (U) - Don’t accept unsolicited jobs online that require you to receive funds from numerous bank accounts and then wire the money to overseas accounts, you could get caught up in a criminal investigation.

(U) How the scheme works:

(U) Typically, you receive an unsolicited e-mail from NACHA, the Federal Reserve, or the FDIC telling you that there’s a problem with your bank account or a recent ACH transaction. (ACH stands for Automated Clearing House, a network for a wide variety of financial transactions in the United States) The sender has included a link in the e-mail for you that will supposedly help you resolve whatever the issue is. Unfortunately, the link goes to a phony website, and once you’re there, you inadvertently download the Gameover malware, which promptly infects your computer and steals your banking information.

(U) After the perpetrators access your account, they conduct what’s called a distributed denial of service, or DDoS, attack using a botnet, which involves multiple computers flooding the financial institution’s server with traffic in an effort to deny legitimate users access to the site, probably in an attempt to deflect attention from what the bad guys are doing.

(U) But that’s not the end of the scheme:

(U) Recent investigations have shown that some of the funds stolen from bank accounts go towards the purchase of precious stones and expensive watches from high-end jewelry stores. The criminals contact these jewelry stores, tell them what they’d like to buy, and promise they will wire the money the next day. So the next day, a person involved in the money laundering aspect of the crime, called a
“money mule” comes into the store to pick up the merchandise. After verifying that the money is in the store’s account, the jewelry is turned over to the mule, who then gives the items to the organizers of the scheme or converts them for cash and uses money transfer services to launder the funds.

(U) In many cases, these money mules are willing participants in the criminal scheme. But increasingly, as part of this scheme, we see an increasing number of unsuspecting mules hired via “work at home” advertisements who end up laundering some of the funds stolen from bank accounts. The criminals e-mail prospective candidates claiming to have seen their resumes on job websites and offer them a job. The hired employees are provided long and seemingly legitimate work contracts and actual websites to log into. They’re instructed to either open a bank account or use their own bank account in order to receive funds via wire and ACH transactions from numerous banks…and then use money remitting services to send the money overseas.

(U) If you think you’ve been victimized by this type of scheme, contact your financial institution to report it, and file a complaint with the FBI’s Internet Crime Complaint Center at www.IC3.gov

(U) SEC Files Charges in Hacking Case (The Wall Street Journal, 27 JAN 2012)

(U) US securities regulators stepped up their battle against hackers in late January, filing civil charges against four firms that allegedly became unwitting enablers of a complex fraud by a Latvian trader. In one of the first cases of its kind, the Securities and Exchange Commission took enforcement action against four US-based electronic trading firms used by the trader as well as charging the alleged hacker himself. The SEC said Igors Nagaicevs, 34 years old, combined hacking with stock manipulation to execute a "brazen and systematic securities fraud" that netted him more than $850,000 in illegal profits. Mr. Nagaicevs couldn't be reached for comment. The SEC filed its action while he was still outside the United States and he has yet to be served with the charges, officials said.

(U) The SEC alleged that Mr. Nagaicevs hacked into the online brokerage accounts of customers at large US broker-dealers more than 150 times between June 2009 and August 2010. Officials declined to disclose those broker-dealers targeted but said they had compensated their customers for the total of more $2 million lost due to the alleged hacking. Mr. Nagaicevs drove the prices of more than 100 stocks up or down by making unauthorized purchases or sales in the "hijacked" accounts, the SEC said. He profited from these artificial price movements by trading the stocks, using the "unfettered" anonymous access to the US markets offered by four online electronic firms, the SEC said.

(U) Officials said the firms should have been registered as brokers but weren't, exposing "US markets to real harm by evading crucial safeguards of the federal securities laws." The trading took place before the SEC last year implemented new rules governing the way broker-dealers allow their customers to trade on US exchanges, which include heightened controls and monitoring of customers' activity. "This case should send a strong message to firms allowing individuals access to US trading markets that they are expected to comply with rules that require such traders to be properly vetted," the deputy chief of the SEC's market abuse enforcement unit, said in an interview.

(U) One of the four trading firms, Mercury Capital of La Jolla, Calif., and its president agreed to settle charges. An associate at Zanshin Enterprises LLC, of Boise, Idaho, another of the trading firms, also agreed to settle SEC charges, though his firm is contesting them. Each agreed to pay a $35,000 penalty, the SEC said. Mercury Capital, which will pay no penalty as part of its settlement, is no longer in business. A lawyer for the associate of Zanshin Enterprises said the modest penalty agreed to by the SEC showed his client "never intentionally allowed the activities alleged against Mr. Nagaicevs." The two
other trading firms: Alchemy Ventures of San Mateo, Calif., and KM Capital Management of Philadelphia, are also contesting the SEC's charges. A lawyer for KM Capital Management and its two co-owners declined to comment. Lawyers for the other firms and executives didn't return calls seeking comment.

(U) The SEC's lawsuit came the same day the Financial Industry Regulatory Authority, a self-regulatory organization that oversees broker-dealers, warned investors of e-mail hack attacks. "Finra has received an increasing number of reports involving investor funds being stolen by fraudsters who first gain access to the investor's email account and then email instructions to the firm to transfer money out of the brokerage account," the alert said. Finra warned investors to check their brokerage accounts for unauthorized transactions and to change their account login information such as their passwords.

(U) Embedded Attacks and Emerging Targets to Dominate 2012 Security Landscape
(www.v3.co.uk, 28 DEC 2011)

(U) McAfee has painted a gloomy security picture for 2012 in which enterprises and criminals shift to new platforms and tactics for securing and infiltrating networks. The company's 2012 Threat Predictions Report said that attacks on industrial systems and embedded hardware will continue as utility companies increasingly use network-connected systems to control infrastructure. The head of research and communications at McAfee Labs, told V3 that the danger of attack on industrial systems could be compounded as hacktivist groups such as Anonymous shift to political protests. "The embedded attacks have been talked about for a while, but it was only in 2011 that it started taking off. There is a lot more discussion going on than ever before," he said.

(U) McAfee also predicts an increase in the use of phony or compromised digital certificates, such as the Diginotar breach, to spread malware and launch targeted attacks. "The targeting of certificate authorities is really damaging. You are really undermining the core trust of the operating system when you abuse the certificate authorities," said the research head. McAfee believes that commercial spam from mailing lists will become more prevalent as companies advertise via email, but that malware and phishing attacks will decline. Many of the major trends from 2011 are expected to carry on into next year, including the rise in mobile malware and the migration of servers to the DNSSEC security standard.

(U) Hackers Expose Defense and Intelligence Officials in US and UK; Security Breach by 'Hacktivists' Reveals Email Addresses of 221 British Military Staff and 242 NATO Officials
(www.guardian.co.uk, 08 JAN 2012)

(U) Thousands of British email addresses and encrypted passwords, including those of defense, intelligence and police officials as well as politicians and NATO advisers, have been revealed on the internet following a security breach by hackers. Among the huge database of private information exposed by self-styled "hacktivists" are the details of 221 British military officials and 242 NATO staff. Civil servants working at the heart of the UK government, including several in the Cabinet Office as well as advisers to the Joint Intelligence Organisation, which acts as the prime minister's eyes and ears on sensitive information, have also been exposed.

(U) The hackers, who are believed to be part of the Anonymous group, gained unauthorized access over Christmas to the account information of Stratfor, a consultancy based in Texas that specializes in foreign affairs and security issues. The database had recorded in spreadsheets the user IDs, usually email addresses, and encrypted passwords of about 850,000 individuals who had subscribed to STRATFOR's
Some 75,000 paying subscribers also had their credit card numbers and addresses exposed, including 462 UK accounts.

An expert in cyber-security at the US Cyber Consequences Unit, a research body in Washington, has analyzed the STRATFOR breach for the Guardian. He has identified within the data posted by the hackers the details of hundreds of UK government officials, some of whom work in sensitive areas. Many of the email addresses are not routinely made public, and the passwords are all encrypted in code that can quickly be cracked using off-the-shelf software. Among the leaked email addresses are those of 221 Ministry of Defense officials, including army and air force personnel. Details of a much larger group of US military personnel were leaked. The database has some 19,000 email addresses ending in the .mil domain of the US military.

In the US case, the cyber-security expert has found, 173 individuals deployed in Afghanistan and 170 in Iraq can be identified. Personal data from former vice-president Dan Quayle and former secretary of state Henry Kissinger were also released. Other UK government departments have been affected: seven officials in the Cabinet Office have had their details exposed, 45 Foreign Office officials, 14 from the Home Office, 67 Scotland Yard and other police officials, and two employees with the royal household. There are also 23 people listed who work in the houses of parliament, including Jeremy Corbyn, Labor MP for Islington North, Lady Nicholson and Lord Roper. Corbyn said he had been unaware of the breach, adding that although his email address was public he was disturbed by the idea that his password could be cracked and used to delete or write emails in a way that "could be very damaging".

Nicholson, speaking on a phone from Iraq, said she had no idea that her personal information had been hacked. She said she was very unhappy that private individuals had had their fundamental right to privacy violated. "To expose civil servants is monstrously unfair," she said. "Officials in sensitive areas like defense and the military could even be exposed to threats. Guarding data like this is extremely difficult, but it's not impossible, and we should do a great deal more."

The hacking has had a big impact because STRATFOR offers expert analysis of international affairs, including security issues, and attracts subscribers from sensitive government departments. The British victims include officials with the Joint Intelligence Organisation (JIO) responsible for assessing intelligence from all sources, including MI6 secret agents. A former deputy head of Whitehall's strategic horizons unit is listed. The unit is part of the JIO based in the Cabinet Office and was set up four years ago to give early warning of potential serious problems that might have an impact on Britain's security or environment.

The extent of the security risk posed by the breach is not known. The cyber-security expert said officials who did not take extra precautions in securing passwords through dual authentication or other protection systems could find email and other databases they use being compromised. "Any foreign intelligence service targeting Britain could find these emails useful in identifying individuals connected to sensitive government activities," he said. British officials, speaking on condition of anonymity, said they were aware of the hacking but it did not pose a risk to national security. Passwords for their communications within Whitehall would be different from any used to access the STRATFOR sites. Whitehall communications would also be protected by extra security walls, officials said. However, they added that their personal communications could be at risk if individuals used the same password as they used to access STRATFOR for their bank accounts and other personal communications.

A government spokesman said: "We are aware that subscriber details for the STRATFOR website have been published in the public domain. At present, there is no indication of any threat to UK government systems. Advice and guidance on such threats is issued to government departments through the Government Computer Emergency Response Team." STRATFOR has taken down its website while it
investigates the security breach. The company says it is "working diligently to prevent it from ever happening again".

(U) This is just the latest action to hit the headlines by hackers associated with Anonymous. The group, whose loose collection of members are scattered around the world and linked through internet chatrooms, has previously targeted Visa, MasterCard and PayPal in protest at the companies' refusal to accept donations for the WikiLeaks website.

(U) Cyber Spies Try Probing US Drone Plans (www.nextgov.com, 03 JAN 2012)

(U) China-based hackers for months have been targeting federal agencies and contractors through infected emails apparently to spy on the Pentagon's drone strategy and other intelligence matters, according to Internet security researchers. The reported espionage employed a tactic known as spear-phishing where infiltrators, operating under the guise of a legitimate sender, email specific victims a virus-laden file or link. In this case, the hackers used email addresses from military and other government organizations, a manager of AlienVault Labs said in January. Some emails went to employees at US military contractors, he said, but declined to discuss any information related to specific victims. The lab traced samples of the malicious software to network addresses in China, AlienVault disclosed last month.

(U) The AlienVault Labs manager has since discovered from the same spies separate malware that is capable of overriding Pentagon smart card credentials, known as the Common Access Card, to get into protected resources. In addition, the intruders have been pursuing other government organizations with information of interest to Chinese intelligence operations, including the General Services Administration, the US government's buying arm, and the Central Tibetan Administration. "After studying all these attacks and all the methods used, we can conclude that they are likely the same group behind all these attacks," he said.

(U) The Chinese government is believed to sponsor cyber strikes on US assets regularly, with the Office of the Director of National Intelligence reporting in November 2011 that "Chinese actors are the world's most active and persistent perpetrators of economic espionage." The thinking is that the authors of the virus are snooping on the US government's plans for remotely piloted aircraft by infiltrating the computers of the aircrafts' designers. "In most of the campaigns the malware dropped displays some document or media attractive to the victim," AlienVault Labs reported in December, 2011. One server consistently sent viruses showing drone images labeled as Defense Department media; computer-generated drone renderings; and Boeing Co. drone prototypes. The campaign appears to have been running since at least September.

(U) This particular malware, called Sykipot, works by injecting itself into a victim's browser or email account and then following orders from the hacker's command-and-control server, the AlienVault Labs manager said. The intruder is capable of ordering the virus to extract documents or insert phony materials, for example. As of December 2011, only a couple of thousand server programs were running these files online and nearly 80 percent of them were located in China, he said. The outsiders apparently tried to hide their footsteps by redirecting commands through hacked US servers. "If someone is seeing that traffic, for instance the security team of the victim organization, it will look less suspicious," he said.

(U) "We shouldn't jump to assumptions but whoever is behind Sykipot is massively collecting information from targeted victims that covers dozens of industries," the manager wrote in December. There are several clues pointing to China. At least six Chinese network locations, or IP addresses, were hosting the command-and-control servers, he found. In addition, one of the tools the authors used to package the email campaigns contained message errors in Chinese. Also, all the documentation to set up
the framework for running the server software is written in Mandarin. And most of the Web addresses displaying the images were registered on Xinnet, a Chinese domain name seller.

(U) This is not the first time cybersecurity researchers have uncovered evidence of a single operative undertaking aggressive surveillance of military contractors. In 2011, McAfee investigators reported that during a targeted five-year operation, one specific entity penetrated the computers of 72 global organizations, including six federal agencies, 13 defense contractors and two computer security companies. Pentagon officials were not immediately able to comment. A GSA spokesman said in a statement, "like every federal agency, we're constantly on the lookout for new attacks against our systems. We've successfully used best-in-class techniques and safeguards to prevent inappropriate access to our systems and continually educate our employees to be on the watch for phishing scams."

(U) Alleged Muscovite Cybercrime Daddy Hauled In To Face US Court (*The Register, 18 JAN 2012*)

(U) A suspected Russian cyber-crook has arrived in the United States to face charges of security fraud, computer hacking and ID theft following his deportation from Switzerland. Vladimir Zdorovenin, 54, of Moscow, Russia, is alleged to have masterminded a series of credit card theft and stock manipulation scams in conjunction with his son, Kirill Zdorovenin, who has not been apprehended. Both were charged in May 2007, long before Zdorovenin senior was cuffed in Zurich last March. He was deported in January just before a scheduled appearance at a Manhattan federal court.

(U) According to the FBI, the duo's stock in trade allegedly involved hacking into computers in order to steal credit card details and brokerage account log-ins. The pair would then allegedly run a series of complicated frauds netting hundreds of thousands of dollars. The FBI said that compromised credit account details, lifted using malware, were used to make fictitious fraudulent purchases to shell companies allegedly established by the suspects, while compromised brokerage accounts were used to purchase shares held by the pair at ramped-up (artificially inflated) prices.

(U) The father-and-son suspects are accused of frauds which targeted US consumers and ran during 2004 and 2005, according to an FBI statement on the case. FBI assistant director Janice K Fedarcyk explains in the statement: "Zdorovenin's egregious behavior illustrated the true colors of the cyber underground, as he and his son allegedly defrauded consumers of hundreds of thousands of dollars using methods that included compromised credit cards, all fronted through fictitious companies they had created. In addition, Zdorovenin allegedly installed malware to access victims' brokerage accounts, trading victims' securities and manipulating the price of stocks Zdorovenin already owned. "This should serve as a stark reminder to anyone who believes he can commit cyber crime and hide behind the safety and anonymity of a Russian IP address; you are not beyond the reach of the FBI," she added. The Russian constitution specifically prohibits the extradition of its citizens, so it is fortunate for the US authorities investigating the case that Zdorovenin strayed into Switzerland.
10K Reasons to Worry About Critical Infrastructure (Wired.com, 24 JAN 2012)

Global Exposure Surface Timeline

(U) Screenshot showing an industrial control system in Idaho that’s connected to the internet. The red tag indicates there are known vulnerabilities for the device that might be exploitable. Two known vulnerabilities are listed at the bottom of the text bubble.

(U) A security researcher was able to locate and map more than 10,000 industrial control systems hooked up to the public internet, including water and sewage plants, and found that many could be open to easy hack attacks, due to lax security practices. Infrastructure software vendors and critical infrastructure owners have long maintained that industrial control systems (ICSes), even if rife with security vulnerabilities, are not at risk of penetration by outsiders because they’re “air-gapped” from the internet, that is, they’re not online.

(U) But a computer science doctoral student at Cambridge University, has developed a tool that matches information about ICSes that are connected to the internet with information about known vulnerabilities to show how easy it could be for an attacker to locate and target an industrial control system. “Vendors say they don’t need to do security testing because the systems are never connected to the internet; it’s a very dangerous claim,” the student said last week at the S4 conference, which focuses on the security of Supervisory Control and Data Acquisition systems (SCADA) that are used for everything from controlling critical functions at power plants and water treatment facilities to operating the assembly lines at food processing and automobile assembly plants. “Vendors expect systems to be on segregated networks — they comfort themselves with this. They say in their documentation to not put it on an open network. On the other side, asset owners swear that they are not connected,” he said. But how do they know?

(U) To debunk the myth that industrial control systems are never connected to the internet, the doctoral student used the SHODAN search engine developed by John Matherly, which allows users to find internet-connected devices using simple search terms. He then matched that data to information from vulnerability databases to find known security holes and exploits that could be used to hijack the systems or crash them. He used Timemap to chart the information on Google maps, along with red markers noting brand devices that are known to have security holes in them. He described his methodology in a paper (.pdf) about the project.
The doctoral student found 10,358 devices connected through a search of two years worth of data in the SHODAN database. He was unable to determine, through his limited research, how many of the devices uncovered were actually working systems – as opposed to demo systems or honeypots – nor was he able to determine in all cases whether the systems were critical infrastructure systems installed at power plants and other significant facilities or simply ICSes that controlled things like high school lighting systems or the heat and air conditioning system in office buildings.

But the student said a few of the systems he investigated did actually belong to water facilities in Ireland and sewage facilities in California. He also found that only 17 percent of the systems he found online asked him for authorization to connect, suggesting that administrators either weren’t aware that their systems were online or had simply failed to install secure gateways to keep out intruders. To avoid obtaining unauthorized access to the systems, the student didn’t try to connect to the systems himself but passed the information to the Department of Homeland Security last September, which took on the task of notifying the owners of systems, where they could be identified, or their ISPs. In the case of systems based overseas, DHS worked with some dozens of CERTs (Computer Emergency Response Teams) in those countries to notify ISPs and device owners.

The doctoral student’s tool shows how easy it is for a dedicated attacker or just a recreational hacker to find vulnerable targets online to sabotage. He told conference attendees that he worked on the tool full time for three months and part time for another three months, noting that if “a student can put this together, surely a nation state can do it.” A conference attendee who works for Schweitzer, a maker of industrial control systems, called the tool “extremely valuable” and said his company had notified customers whose systems were found online. “At least one customer told us ‘We didn’t even know it was attached’,“ he said.

The doctoral student is not the first to use SHODAN to uncover ICSes connected to the internet. Last February, an independent security researcher used SHODAN to identify online remote access links to SCADA systems at multiple utility companies. But he is the first to show how easy it would be for attackers to automate device location information with vulnerability and exploit data. He used 33 queries to find the devices online, using the names of popular industrial control systems such as “SoftPLC,” a control system used primarily in Eastern Europe, and “Simatic S7,” a system made by Siemens that was targeted last year by the Stuxnet worm in an attack aimed at sabotaging Iran’s uranium enrichment program.

Using banner information that is broadcast by each connected system, such as the date and timezone, which can help place a machine geographically, as well as the type and version of servers and devices being used, the doctoral student searched databases for information about patched and unpatched vulnerabilities (including a list of new vulnerabilities that a group of researchers exposed in six industrial control systems at the S4 conference) as well as known exploits to attack those systems. Then he plugged the data into his visualization tool. Without trying to access the ICSes, he was unable to determine if the devices that were found are patched, and therefore not vulnerable to the existing exploits, or if they are protected by intrusion prevention systems.

Smart Grid Security Inadequate, Threats Abound (IDG News Service, 04 JAN 2012)

Near chaos. That's the current state of security for smart grids, according to Pike Research. A recent report by the research firm finds that a lack of security standards, a hodgepodge of products and increasingly aggressive malicious hackers will make 2012 a challenging year for securing smart grids. (A smart grid uses IT and smart meters in an effort to make electric utilities more efficient, reliable and sustainable.) "After years of vendors selling point solutions, utilities investing in compliance minimums rather than full security, and attackers having nearly free rein, the attackers clearly have the upper hand.
Many attacks simply cannot be defended," says an analyst at Pike Research. But he adds: "There is hope." The analyst says there's a "dawning awareness by utilities during the past 18 months of the importance of securing smart grids with architecturally sound solutions."

(U) A smart-grid pioneer, former CIO at Austin Energy, and co-author of The Advanced Smart Grid: Edge Power Driving Sustainability, says security is a complex situation. He notes that a fully secure smart grid requires secure edge devices, secure networks, secure data centers and secure applications. Looking at the current state of affairs, the former CIO says "security from the application data center to the utility sub-station is pretty good." However, he says "security from edge devices back to the sub-station and/or data center needs a lot of work."

(U) The hackers aren't waiting. "Development of cybersecurity solutions and standards has somewhat stalled, while the attackers are steaming ahead at full speed," the Pike Research analyst says. "While we do have lots of good point solutions available," he says, "they are just that: point solutions." The problem is that hackers find the gaps between those products. He says that, outside of defense agencies, it's rare to find a utility with a well-planned smart grid security program that integrates those products into a working whole.

(U) There's also a danger of overlooking the insider threat. "Most people believe smart grid security is for only viruses and worms from hostile governments and terrorist groups," says an analyst at ABI Research. "However, one of the main reasons for increased spending on smart grid security software and management systems is simply to make sure the correct people have access to the equipment and systems they should have access to." Among other things, this means protecting systems from disgruntled employees or others who might commit internal sabotage, Flood says.

(U) Security Standards Need Teeth

(U) The Pike Research report suggests that the lack of enforceable security standards or regulations for power distribution grids "leads to a scene of mass chaos in utility cybersecurity" and will cause utilities to take a wait-and-see approach to significant security investments. So far, most utilities are focusing on the North American Electric Reliability Corp.'s critical infrastructure protection program (NERC CIP), which applies only to generation and transmission and is the only current standard that has "the teeth to result in fines for noncompliance," the report says.

(U) But utilities should look beyond regulatory compliance and take a more holistic, risk assessment approach, analysts say. Utilities need to establish (and continually refine) an "organization-wide risk management program, policies and processes to prepare for, react to, and recover from adverse cybersecurity events," says a senior advisor for information system security at the National Institute of Standards and Technology (NIST). NIST and other government agencies have written useful documents about power grid security and risk management, but the Pike Research report notes that they are merely recommendations.

(U) To complicate matters further, there are differences between the security standards in the United States and the rest of the world, the ABI Research analyst says. "We need similar standards worldwide, and although organizations such as the European Union's Smart Grid Coordination Group are working with NIST closely, we still need greater progress in Europe on smart grid security," he says. "However, with current economic problems in the euro zone, less effort and time will be spent on the smart grid than needed."
Securing industrial control systems such as SCADA (supervisory control and data acquisition) also remains a challenge for utilities, according to the Pike Research analyst, but there is little agreement about what to do about it. A major factor, he explains, is that many SCADA systems were deployed without any security whatsoever in the mistaken belief that SCADA would always be isolated from the Internet. "Even when it is, attacks such as Stuxnet can circumvent the isolation by using USB memory sticks to spread," he says. He adds that SCADA networks can have many old serial protocol devices that have no hope of running any security software, let alone producing event logs for forensics.

Technical Fix for Security Risks?

"There are lots of good technologies available now but none is a silver bullet," the Pike Research analyst says. "As with any environment, security requires risk assessment, policies, and an architecture before you start specifying products." That said, he lists five promising technologies for utility cybersecurity over the next few years:

- Multi-factor authentication: This will help ensure that a stolen password is not enough to allow an attack against a grid or a control console from the other side of the world.

- Control network isolation: A firewall can make sure that enterprise IT traffic does not end up on the utility's control network.

- Application white-listing: White-listing prevents the execution of malware by identifying "a list of permitted actions on a host and allows nothing else," says the Pike Research report.

- Data encryption at rest and in transit: This approach not only protects data confidentiality, it also helps ensure the integrity of data from devices such as smart meters, temperature sensors and flow meters.

- Event correlation: This can be especially useful for identifying the source of attacks and in some cases preventing them.

People Biggest Security Problem

Perhaps the biggest security hurdle facing utilities is the cultural divide between IT teams and utility operations teams, says the Pike Research analyst. "One side understands how enterprise IT networks operate," he says. "The other side understands how distribution and transmission grids function. There is not that much overlap between the two, but each has the opportunity to make the other's life truly miserable." Lockhart observes that the most progressive utilities have realized that cybersecurity discussions must include both IT experts and operations experts, but other utilities are lagging in this regard. "From my research, there are still some utilities where those two teams are not on speaking terms," he says. "Many security vendors tell me that when they visit utilities, they are only seeing the CIO or chief security officer."
(U) SCADA Systems in Railways Vulnerable to Attack (EWeek, 25 JAN 2012)

(U) Reports of a possible cyber-attack against a rail company highlight the issues of protecting industrial control systems that keep the country's critical infrastructure running. Government officials initially believed railway signal disruptions in December were tied to a cyber-attack against a Northwest rail company in December, Nextgov reported. But government and railway officials later denied that a US railroad had actually been hit by a cyber-attack. "There was no targeted computer-based attack on a railroad," said a spokeswoman for the Association of American Railroads.

(U) While an attack has been ruled out, the incident highlights the dangers of industrial control systems controlling critical infrastructure. Train service on the unnamed railway was "slowed for a short while" and schedules delayed for 15 minutes on Dec. 1, according to a Transportation Security Administration memo obtained by Nextgov. A "second event" occurred just before rush hour the next day, but it did not affect schedules, according to the Dec. 20 memo, which summarized the agency's outreach efforts to share threat intelligence with the transportation sector. "Amtrak and the freight rails needed to have context regarding their information technical centers," the memo said, adding that rail operators were not focused on cyber-threats.

(U) TSA investigators discovered two IP addresses for the intruders associated with the Dec. 1 incident and another for Dec. 2. Investigators considered the possibility of the attackers being based overseas, but did not specify the suspected country, Nextgov reported. Alerts listing the three IP addresses were sent to several hundred railroad firms and public transportation agencies. Officials at the Department of Homeland Security, which oversees the TSA, told Nextgov on Jan. 23 that further investigation showed it may not have been a targeted attack, but did not explain what may have caused the "anomalous activity."

(U) The railway incident is similar to what happened at an Illinois utility last fall. A government fusion center claimed Russian attackers had remotely destroyed the facility's water pump, but the DHS on further investigation claimed it was not an attack. It later turned out the intrusion had been an American contractor remotely logging in to perform some maintenance tasks.

(U) However, the TSA's railway memo highlights how vulnerable the railways are to an attack on supervisory control and data acquisition (SCADA) systems, according to experts from Casaba Security, a security analysis and consulting company. Just about anything in the railway infrastructure could be controlled by SCADA systems, including track switches, signal and crossing lights, transformers, weather and track sensors, engine monitors, railway car sensors, electronic signs and even turnstiles, said Casaba's co-founder. Most of these systems are connected to the network so that they can obtain data collected by the sensors. "A sensor that can detect the position of a track switch is not helpful unless it can pass that data to an operations center hundreds of miles away," he said.

(U) Connecting SCADA systems to the Internet puts the infrastructure at risk because it opens up the possibility of intruders finding a way into the network. However, many organizations take that risk to save money, simplify the infrastructure and ease maintenance. It is usually cheaper to transmit data over the Internet instead of investing in dedicated lines or wireless frequency space, according to Casaba's president. "The benefit of SCADA being 'online' is that the Internet is cheap, robust, standardized and easily accessible," he said.

(U) The downside is that without proper protections, the infrastructure is wide open to anyone looking. A Cambridge University researcher developed a tool that mapped more than 10,000 industrial control systems accessible from the Internet, including water and sewage plants. While some of the systems could have been demo systems or used in places that wouldn't count as critical infrastructure, such as the
heating system in office buildings, some were active systems in water facilities in Ireland and sewage facilities in California.

(U) Only 17 percent of the systems mapped asked for authorization to connect, suggesting that administrators either weren't aware the systems were online or had not installed secure gateways, the Cambridge researcher said. A computer science doctoral student at Cambridge, he presented the findings at the S4 conference in Miami. Administrators need to set up secure and isolated networks and use Secure Sockets Layer or a virtual private network to restrict who can talk to the controllers, according to the chief scientist at Casaba. Since SCADA systems will likely be Internet-accessible, administrators should focus on putting them behind a secure gateway. "Increasingly all the communications are over the Net, so being on the Net is all but inescapable," he said.

(U) COUNTERTERRORISM THREAT ITEMS FROM THE PRESS:

(U) Appeals Court Upholds Convictions in Fort Dix Plot (The Associated Press, 28 DEC 2012)

(U) A federal appeals panel in late December upheld the convictions and sentences of five Muslim men accused of planning to attack Fort Dix or other military bases, though it threw out a charge against one defendant. The main issue was prosecutors' use of wiretaps obtained under the Foreign Intelligence Surveillance Act, a part of the Patriot Act aimed largely at gathering foreign intelligence. The recordings were a major piece of a 2½-month trial for the five men, all Muslim immigrants who grew up in the New Jersey suburbs of Philadelphia. The men: Mohamad Shnewer, Serdar Tatar, and brothers Dritan, Eljvir and Shain Duka were arrested in May 2007. In 2008, a federal jury in Camden, New Jersey, convicted them of conspiring to kill US military personnel at Fort Dix. All but Tatar are serving life terms.

(U) Defense lawyers said it was unconstitutional to use the recordings in a domestic criminal case and that it may have been impossible to convict the men without the evidence. But in a unanimous ruling written by Judge Marjorie O. Rendell, a three-judge panel of the Philadelphia-based 3rd US Circuit Court of Appeals disagreed. The challenged search "was conducted in objectively reasonable reliance on a duly authorized statute," and therefore admissible at trial, Rendell wrote.

(U) Another major issue came from an error that federal prosecutors acknowledged in January: Three of the men were convicted of attempted possession of firearms in furtherance of a crime, but the law in question does not have a provision that outlaws attempted possession. In the case of that count against Dritan and Shain Duka, the judges said defense lawyers should have raised it before the trial judge. Since they didn't, the judges said, it should not be overturned. The judges also said that there was evidence at trial that the two actually possessed weapons. But the case of Shnewer was different. The court ruled that there was no evidence he possessed the weapons. As a result, his weapons conviction was dismissed, along with the 30-year prison term that went with it. He is still serving a life term.
(U) Maryland Man Admits Plotting Terror Attack on Military Recruiting Center (Fox News, 26 JAN 2012)

(U) A Maryland man pled guilty in January to trying to detonate what he thought was a car bomb outside a military recruiting center in suburban Baltimore, saying he was motivated by what he saw as an American war on Islam. Antonio Martinez, 22, admitted trying to use a weapon of mass destruction to blow up an Armed Forces recruiting center in Catonsville in December 2010. He faces 25 years in prison over the foiled plot after coming to an agreement with prosecutors, the Baltimore Sun newspaper reported. Martinez, a US citizen who was born abroad, preferred to be called Muhammad Hussain after converting to Islam and signed the plea using both names. Public records are unclear about when Martinez, a former part-time construction worker, moved to Maryland, but he attended Laurel High School in Prince George's County.

(U) Martinez was arrested on Dec. 8, 2010, after he attempted to detonate what he believed to be explosives, supplied by federal agents, at the recruiting center. His lawyer previously claimed that his client had been entrapped and that the bombing plot was designed by the federal government to set up Martinez. He allegedly wrote about his support of jihad (holy war) and his desire to go fight in Afghanistan or Pakistan on Facebook, in the months before the foiled attack, according to an FBI informant. "My dream is to be amongst the ranks of the mujahideen," Martinez allegedly wrote. "Jihad is all I think about when i sleep, when I wake up, sometimes i cry cuz im not there and kaffur [nonbelievers] killing all our brothers and sisters." Martinez allegedly told the informant in October 2010 that he wanted to "kill them as they killing muslim around the world," an FBI email said.

(U) Martinez decided on a car bomb after a discussion with the undercover agent because "using a bomb would allow him to commit further acts here and overseas," prosecutor Christine Manuelian said. The informant and the undercover agent gave Martinez repeated opportunities to back out, but he insisted he was committed, even after expressing reservations after a Somali-born teenager was arrested in Oregon in a similar sting, according to court documents. He will be sentenced April 6 at Maryland US District Court.

(U) Muslim Man from Kosovo Charged in Florida Bomb Plot (The Associated Press, 09 JAN 2012)

(U) Kosovo-born Muslim man was charged with plotting to attack crowded locations around Tampa, including nightclubs and a sheriff's office, with a car bomb, assault rifle and other explosives, federal authorities said in January. According to a federal complaint, 25-year-old Sami Osmakac recorded an eight-minute video shortly before his arrest explaining why he wanted to bring terror to his "victims' hearts" in the Tampa Bay area. Osmakac is a naturalized American citizen born in Kosovo, then part of the former Yugoslavia in eastern Europe.

(U) In the video, Osmakac is seen cross-legged on the floor with a pistol in his hand and an AK-47 behind him. Osmakac said in the video that Muslim blood was more valuable than that of people who do not believe in Islam, according to the complaint. He said he wanted "payback" for wrong that was done to Muslims, the complaint said. There is no indication that Osmakac planned to attack the Republican National Convention, which will be held in Tampa in August, federal authorities said.

(U) The area's Muslim community helped provide authorities with information, said the special agent in charge of the FBI's Tampa division. "This case is not about the Muslim religion and it's not about the Muslim community," he said. "It's about an individual who committed a crime." Osmakac gave only brief answers to basic questions during his first appearance in federal court. He wore a blue jail outfit and was shackled at his wrists and ankles. His public defender declined to comment afterward. A US Magistrate
Judge ordered Osmakac held without bail. If convicted on the single count of attempted use of a weapon of mass destruction, Osmakac could face life in prison.

(U) Osmakac was arrested after he allegedly bought explosive devices and firearms from an undercover agent. The firearms and explosives were disabled by law enforcement before the sale. Osmakac lived with his parents in a tan stucco home in Pinellas Park, Fla., a small city west of Tampa. He worked occasionally at the Balkan Food Store and Bakery in St. Petersburg, a small store owned by his parents. According to public records, Osmakac had one prior brush with the law. In April 2011, Tampa Police said Osmakac, dressed in "what appeared to be traditional Middle-Eastern attire with a small cloth" on his head, got into an argument over religion outside a Lady Gaga concert in downtown Tampa. A police report said anti-gay protesters outside the concert saw Osmakac driving by in a truck and turned their attention to him because of his appearance. "The protesters began verbally berating the man and the Muslim faith and their attacks became personal and nasty," wrote a Tampa police officer. The report said Osmakac parked his vehicle, walked up to the protesters and got into an argument with one man who insulted Allah, Mohammed and the Quran. Osmakac was accused of head butting one man and was charged with battery, although Krupa noted that the protesters were "not promoting peace or tolerance, but rather of inciting violence and hate." That case had not yet been resolved, according to court records.

(U) Federal officials say Osmakac's new charges stem from information given to them by a confidential source in September 2011. According to the federal report, Osmakac walked into the source's business looking for al-Qaida flags. The confidential source then hired Osmakac and was in constant contact with federal officials and audio or video taped their conversations. Two months later, the federal complaint said, Osmakac and the confidential source discussed and identified potential targets in Tampa that Osmakac wanted to attack. Osmakac allegedly asked the source for help getting firearms and explosives for the attacks, and the source put him in touch with an undercover FBI employee.

(U) On Dec. 21, Osmakac met with the undercover agent and allegedly told the agent that he wanted to buy an AK-47-style machine gun, Uzi submachine guns, high capacity magazines, grenades and an explosive belt. During a later meeting, Osmakac gave the agent a $500 down payment for the items. Osmakac also asked the undercover employee to build bombs that could be placed in three different vehicles and detonated remotely, the US Justice Department said in a press release. Osmakac then planned to follow up with an attack using the other weapons he asked for, authorities said.

(U) On Jan. 1, Osmakac told the agent he wanted to bomb nightclubs, the operations center of the Hillsborough County Sheriff's Office and a business in Tampa. Osmakac told the undercover FBI agent that he wanted to detonate a car bomb and use the explosive belt to "get in somewhere where there's a lot of people" and take hostages. Osmakac told the agent that after he took hostages he wanted to demand something from the "kuffar" — an Arabic word that means infidels or disbelievers of Islam, federal authorities said.

(U) According to the affidavit, he also said, "Honestly, I would love to go for the Army people, but their bases are so locked up, I have to do something else." Osmakac said he wanted to take down the bridges that link Tampa to neighboring Pinellas County. "This will crush the whole economy," he allegedly said to the agent. "This would crush everything man, they would have no more food coming in. They would, nobody would have work." During that meeting, the agent told Osmakac he could always change his mind about his plot. "According to the complaint, Osmakac immediately shook his head in the negative and stated, 'We all have to die, so why not die the Islamic way?'" according to the press release.

(U) Analyst Comment: According to court documents, Osmakac intended to attack military personnel, but shifted his planning to nightclubs and possibly bridges because military targets are too difficult to

UNCLASSIFIED

51
attack and attacking bridges would have an economic impact. Security personnel of both military and government facilities and commercial sector businesses should be aware of the indications of pre-operational attack planning and surveillance, as this suspect based his attacks not only on the level of security, but also the impact of the attack. Any suspicious activity should be reported to local law enforcement immediately.

(U) Colorado Man Arrested On Terrorism Charges (The Associated Press, 23 JAN 2012)

(U) The FBI arrested a refugee from Uzbekistan at Chicago's O'Hare airport on charges that he planned to travel overseas to fight for a terrorist group and give up his life if necessary, an official said in January. However, there was no evidence that suspect Jamshid Muhtorov was plotting attacks inside the United States, authorities said. Muhtorov, 35, of Aurora, Colo., was arrested by members of the FBI's Denver and Chicago Joint Terrorism Task Forces.

(U) Muhtorov, who goes by several other names, was indicted for providing and attempting to provide material support to a designated foreign terrorist organization. Prosecutors allege he planned to fight for the Islamic Jihad Union, which has been blamed for suicide attacks in Uzbekistan and claimed responsibility for numerous attacks against coalition forces in Afghanistan. Muhtorov was arrested without incident before he could board a flight to Istanbul, Turkey, said a spokesman for the US Justice Department in Washington.

(U) Muhtorov made a brief court appearance in Chicago and waived his rights to further hearings in the northern Illinois district. Judge Morton Denlow then ordered Muhtorov to be transferred to Denver but it wasn't immediately clear how soon that would happen. Investigators obtained a search warrant for Muhtorov's apartment for a laptop computer, a Blackberry cell phone, and permission to search two email accounts they said were used by Muhtorov, according to the indictment. The FBI said Muhtorov communicated with a contact with the terror organization by email using code words, asking to be invited to the "wedding." He also told the contact that he was "ready for any task, even with the risk of dying," the FBI said.

(U) Neighbors said Muhtorov worked as a truck driver and lived with three children and a woman. A neighbor said a white, unmarked 18-wheeler truck was often parked outside the building. He said he saw Muhtorov and his family out barbecuing once a week, but he didn't talk to him. Another neighbor said people he assumed were in law enforcement were in and out of Muhtorov's apartment much of the day of the arrest. If convicted, Muhtorov could face a maximum sentence of 15 years in prison, and up to a $250,000 fine.

(U) It wasn't the first terrorism case with ties to the Denver suburb of Aurora. Najibullah Zazi, a Denver airport shuttle driver who pleaded guilty to planning to bomb the New York City subway, also was from Aurora. Zazi, an Afghan immigrant, bought beauty supplies in Aurora to make peroxide-based bombs. He tried to mix explosives in a hotel room in the city then drove to New York to carry out an attack just before the 2009 anniversary of the Sept. 11 attacks. After becoming suspicious he was being watched by law enforcement, he abandoned the plan and returned to Colorado. Prosecutors allege Zazi and two associates went to Afghanistan in 2008 to join the Taliban and fight US soldiers. They instead were recruited by al-Qaeda operatives, who gave them weapons training in their Pakistan camp and asked them to become suicide bombers, authorities say. Zazi's father, Mohammed Zazi, also of Aurora, was convicted in July of destroying evidence and lying to investigators to cover up his son's plot.
(U) Three Men Sentenced In North Carolina Terrorist Ring (CNN, 13 JAN 2012)

(U) -- Three men received sentences in January ranging from 15 to 45 years for their roles in a homegrown terrorism ring based in North Carolina. Hysen Sherifi, a native of Kosovo and a legal permanent resident of the United States, was sentenced to 45 years in prison. Ziyad Yaghi, a naturalized US citizen, got almost 32 years. The two men were convicted in October of plotting to kill people overseas and of conspiracy to provide material support for terrorism. Sherifi also was convicted of conspiring to kill a federal officer or employee and of two firearms charges. The third man, Mohammad Omar Aly Hassan, was sentenced to 15 years behind bars for conspiracy to provide material support to terrorism. All three are in their 20s and had pleaded not guilty.

(U) The men were part of a ring that prosecutors said was thought to comprise eight people. The leader, Daniel Patrick Boyd, pleaded guilty in February to conspiracy to kill people overseas and of material support for terrorism. He has not been sentenced. Sherifi and Boyd had discussed attacking the Quantico, Virginia, Marine Corps base. According to prosecutors, Boyd was a convert to Islam who had received training in terrorist camps in Pakistan and Afghanistan. Boyd recruited and trained others to go overseas and undertake violent jihad. According to the indictment charging the men, they believed that such violence was an obligation and decided "should their efforts to fight jihad overseas prove impossible, jihad would take place here in the United States."

(U) The indictment said that from November 2006 through July 2009, Boyd conspired with the others to provide material support to terrorists. That included money, training, transportation and manpower. Boyd and most of the others were arrested and charged in July 2009. Two of his sons, Zakariya and Dylan Boyd, pleaded guilty to conspiracy to provide material support to terrorism this year and received sentences of nine and eight years, respectively. Anes Subasic, a naturalized US citizen, is awaiting trial in North Carolina. The eighth suspect charged in the case is Jude Kenan Mohammad, a US citizen who authorities say is believed to be at large in Pakistan.

(U) In April 2010, a ninth man was charged in what previously had been known as an eight-person conspiracy. Bajram Asllani, a resident of Kosovo, was charged with conspiracy to kill people overseas and to provide material support to terrorists. The government alleges that Asllani solicited money from Boyd and the others to establish a base of operations in Kosovo to carry out violent jihad. He is reportedly at large in Kosovo.

(U) Feds Say Michigan Company Has Ties to Terrorist (HometownLife/The Observer, 29 DEC 2011)

(U) According to federal prosecutors, a nondescript shipping company in Redford, Michigan played a major role in funding the terrorist organization Hizballah. "The intricate scheme laid out in (this) complaint reveals the deviously creative ways that terrorist organizations are funding themselves and moving their money, and it puts into stark relief the nexus between narcotics trafficking and terrorism," said US Attorney for the Southern District of New York Preet Bharara. "We are putting a stranglehold on a major source of that funding by disrupting a vast and far-flung network that spanned three continents."

(U) The Department of Justice recently filed a 66-page criminal complaint in New York that outlined what prosecutors say was an intricate money laundering operation that funneled millions of dollars to Hizballah, a group based in Lebanon that the US State Department classifies as an Iranian-supported terrorist organization that was behind the April 18, 1983, bombing of the US Embassy in Beirut, Lebanon. Named in the complaint is Oussama Salhab, owner of Cybamar Swiss LLC, a car transport company headquartered in Redford Township at 12130 Dixie
(U) Federal probe

(U) Federal authorities allege that over $1 billion in used cars were purchased and shipped overseas for resale with profits going to support Hizballah. And many of the cars were shipped by Cybamar. According to the complaint, 208 wire transfers totaling over $13 million in United States currency were routed through Cybamar bank accounts, over $10 million from one account at a Detroit Comerica branch. On the company website, Cybamar Swiss says its "worldwide presence makes us your number one choice for international logistics. Whether you are shipping a vehicle to Nigeria, moving to Dubai or Abu Dhabi, or transporting freight to anywhere in Africa, Europe and the Middle East, we are here to help."

(U) Salhab left the United States and Cybamar officials had no comment. Salhab was born in the Bekaa Valley, Lebanon, and currently resides in Togo and Lebanon. Federal prosecutors have named Salhab as a "Hizballah operative" and say he flew into Detroit Metropolitan Airport on a flight from Beirut on Nov. 22, 2009. During an interview with a US Customs and Border Protection officer, Salhab stated that he was traveling to the United States for business on behalf of Cybamar Swiss. He had a finger-print encrypted laptop that contained images of Hizballah Secretary General Hassan Nasrallah; audio of the Hizballah anthem; images of Hizballah militants stomping on an Israeli flag; and movie files of executions, hangings, torture, and beheadings. Salhab claimed that the images were placed on his computer by an employee. Salhab was allowed to withdraw his application for admission into the United States, and departed the country. Prosecutors say Salhab is heavily involved in the used car business and controls a network of money couriers who have transported millions of dollars in cash from West Africa to Lebanon, and who have traveled to the United States to transport cash and to purchase used cars for shipment to West Africa.

(U) Drug connections

(U) The complaint alleges that Salhab and his company, Cybamar, was a link in a huge operation that also included the Hassan Ayash Exchange Company, the Ellissa Exchange Company, and other Lebanese financial institutions, including Middle East and Africa Bank and the Federal Bank of Lebanon and BLOM Bank. A second Redford company, United Auto Exchange Enterprise, 12130 Dixie Suite B, is also listed in the complaint. The car buyers in the United States typically had little or no property or assets other than the bank accounts used to receive the overseas wire transfers. A significant portion of the cash proceeds from the car sales was transported to Lebanon by a Hizballah-controlled system of money couriers controlled by Salhab.

(U) Prosecutors said the same money laundering infrastructure was used to conceal and funnel hundreds of millions of dollars in narcotics proceeds from West Africa back to Lebanon. The complaint seeks the assets of Cybamar, many banks, approximately 30 US car buyers and civil money laundering penalties totaling $483,142,568, which represents the sum of the funds laundered."... The connection between drug traffickers and terror networks is evident. By attacking the financial networks of those who wish to harm innocent Americans, DEA is strengthening national security and making our citizens safer," said DEA Administrator Michele M. Leonhart.

(U) Analyst Comment: This article focuses on the threat that criminal activity, such as money laundering and activity that appears legitimate, such as shipping automobiles to overseas destinations, may be used to support terrorist fundraising. Information on fundraising through export shipping or imports of counterfeit items should be reported to the FBI.
(U) Analysis: Al Qaeda vs. the West: 2012 and Beyond ([www.cnn.com](http://www.cnn.com), 27 DEC 2011)

(U) Mitchell D. Silber is the author of 'The Al Qaeda Factor: Plots Against the West'. He is also the Director of Intelligence Analysis for the NYPD. His thoughts do not necessarily represent the opinions of the New York City Police Department.

(U) Just over two years since al Qaeda Core launched the most serious plot on American soil since 9/11 (the Najibullah Zazi NYC Subway Plot of September 2009), al Qaeda’s leader and founder Usama bin Laden, al Qaeda’s most recent “Number 3” Attiyah Abd al Rahman, and the al Qaeda instigators of the Zazi Plot – Saleh al Somali and Rashid Rauf – are all dead - a result of a combination of efforts by US Special Forces and drone strikes. In addition, this fall, Anwar al Awlaqi, al Qaeda in the Arabian Peninsula’s dual-hatted English language propagandist and chief of external operations, was also killed in a drone strike. The natural question to ask, as the calendar approaches 2012, is: wither the al Qaeda threat?

(U) The recent past may provide some useful insights. One of the most important findings of a forensic study of the sixteen most serious al Qaeda plots against the West since 1993 is that al Qaeda plots against the West are almost always underpinned and manned by Westerners - who travel overseas to al Qaeda or an al Qaeda ally/affiliate and then are turned around opportunistically and sent back to target the West. Whether it was the 1999 LAX Millennium Bomber (Montreal), 9/11 Pilots (Hamburg), Shoe Bombers (London), July 7 and 21 2005 London transit system bombers (Leeds and London), 2009 NYC Subway Bombers (New York) or 2009 Underwear Bomber (London), the key operatives from the plot originated in one of the great cities of the West.

(U) The effort by radicalized Americans to travel abroad and join up with al Qaeda affiliated terrorist groups has continued unabated since 2001. To name just a few, this group includes Bryant Neal Vinas and Adam Gadahn (al Qaeda Core), Samir Khan (AQAP), Omar Hammami, Zachary Chesser and nearly two dozen men from Minneapolis (al Shabaab), David Headley (Lashkar-e-Taiba), Abdul Hameed Shehadeh (unnamed jihadist groups in Pakistan) and Betim Kaziu (jihadist groups in either Iraq or the Balkans), to name just a few. This begs the question, what hot spots might men who radicalized to violence in London, the Washington DC suburbs, New York City or Toronto travel to in order to carry out their jihadist ambitions in 2012 and beyond?

(U) Af/Pak: Al Qaeda Core remnants and Pakistani jihadist groups

(U) Although key members of al Qaeda Core’s leadership have been removed from the battlefield, Ayman al Zawahiri and Adnan el Shukrijumah, a key orchestrator of the 2009 NYC Subway Plot, remain alive in the borderlands of Afghanistan and Pakistan. Any Westerners who might find their way upstream and receive training would surely provide a tempting means by which al Qaeda Core could attack the United States. However, a potentially greater threat than a unilateral al Qaeda attack would be one originating from the blending of Pakistani jihadist groups who have safe havens to operate from, robust operational capabilities, and are willing to subcontract for al Qaeda Core. A prime example of this is the case of David Headley. In his plot targeting Copenhagen, Denmark in 2008, Headley did reconnaissance for Lashkar-e-Taiba (LeT) on the Jyllands Posten newspaper’s headquarters. LeT lost its interest in targeting Jyllands Posten directly and dropped out of the plot after carrying out the Mumbai attacks of November 2008. Headley and his chief operational officer Ilyas Kashmiri then shopped the plot and the reconnaissance work to al Qaeda Core, who was interested in leveraging it. The result was a series of warnings throughout the fall of 2010 in Western Europe regarding a “Mumbai-style al Qaeda plot”.

UNCLASSIFIED

55
(U) There is an entire alphabet soup of Pakistani jihadist groups with whom al Qaeda Core could partner to target the United States, including the Haqqani network, Jaish-e-Mohammed (JeM), Harkat ul Mujahideen (HuM), Tehreek-e-Taliban (TTP), and LeT, to name a few. And, as Pakistani-US relations continue to deteriorate, there is an increased likelihood of a Pakistani jihadist group seeking to target US interests, potentially even as a form of asymmetrical warfare.

(U) Somalia and Yemen: An Alliance of AQ Franchises

(U) Another blended threat incorporates two al Qaeda affiliates: al Shabaab in Somalia with al Qaeda in the Arabian Peninsula (AQAP). For more than twenty years, Somalis seeking relative refuge from the strife and famine in their broken country have crossed the Arabian Sea to Yemen. However, this human traffic has also enabled coordination between the two terrorist groups, as the arrest of Ahmed Warsame in 2011 has proven. The Southern District of New York described Warsame in its indictment as a conduit between al Shabaab and al Qaeda in the Arabian Peninsula, who provided AQAP with material support “in the form of money, training, communications equipment, facilities, and personnel while he was in Yemen in 2010 and 2011.” This comingling of al Qaeda affiliates and allies is especially worrisome considering that more than fifty Americans, Canadians and British citizens have traveled to Somalia to join al Shabaab and could serve as some of the “personnel” provided to AQAP for training and/or redeployment.

(U) Sub-Saharan Africa: Another Transnational AQ Alliance

(U) Although it is further off the radar of most Western terrorism analysts, there is a new frontier where an al Qaeda-type threat is metastasizing: Nigeria. The group, Boko Haram, has seen a significant increase in capabilities due to coordination with other al Qaeda affiliates and allies, in particular al Shabaab and al Qaeda in the Islamic Maghreb (AQIM). Until this summer, Boko Haram had focused primarily on domestic issues; now it has the potential to project power abroad against US targets. Boko Haram’s August 2011 vehicle-borne improvised explosive device attack on the UN headquarters in Abuja marked a striking departure for the group from indigenous to international targets. Expressing his concern over Boko Haram’s nascent collaboration with Al Shabaab and AQIM, US Army General Carter Ham, Commander of AFRICOM, told reporters in Washington this past September, "If left unaddressed, you could have a network that ranges from East Africa through the center. Those three organizations have very explicitly and publicly voiced intent to target Westerners and the United States specifically. To me, that is very, very worrying."

(U) The Homeland: New York, Baltimore, Seattle, Dallas etc...

(U) The last twelve months have seen a significant increase in the number of Americans who radicalized to violence and decided that rather than travelling abroad to carry out their jihadist ambitions, they could conduct attacks at home. Whether it was Mohammed Osman Mohammed targeting the Portland Christmas tree lighting ceremony, Antonio Martinez targeting a Baltimore area military recruiting facility, Ahmed Ferhani and Mohamed Mamedouh targeting a Manhattan synagogue or Jose Pimintel building a bomb in an apartment in Washington Heights in Manhattan, "do it yourself" (DIY) terrorism, inspired by al Qaeda seems on the ascent in the homeland. In fact, Inspire Magazine has advised "would be warriors" from the West to avoid international travel and carry out attacks at home. Micro-conspiracies like these are extremely difficult to detect and disrupt before it is too late. Unfortunately, they have increasingly become an extension of the al Qaeda threat.
The al Qaeda threat of 2012 and beyond is a disaggregated one that is made up of horizontal networks, nodes and hubs of al Qaeda affiliates and allies. As al Qaeda Core’s power continues to diminish, other nodes in the network will rise in power and stature to launch plots against the West just as AQAP and TTP in 2009 did in 2009 and 2010. Although the path to al Qaeda Core may not be as attractive as it once was to men from Montreal, London, New York or Hamburg, in 2012 and beyond, new frontiers have opened for those “would be warriors” radicalized in the West who seek to carry out their jihadist ambitions overseas. Counterterrorism officials, policymakers and intelligence and police agencies dare not let their guard down in 2012.


US-born al Qaeda militant Anwar al-Awlaki, killed in a CIA drone strike in September, posthumously called on US Muslims to join the group in the Middle East in a video released on in December. Awlaki, identified by US intelligence as "chief of external operations" for al Qaeda's Yemeni branch and a web-savvy publicist for the Islamist cause, was killed in a remote Yemeni town by missiles fired from multiple CIA drones.

"You have two choices: either hijra (emigration) or jihad (holy war)," Awlaki said in the video, which was posted on Islamist websites. "I specifically invite the youth to either fight in the West or join their brothers in the fronts of jihad: Afghanistan, Iraq, and Somalia. "I invite them to join us in our new front, Yemen, the base from which the great jihad of the Arabian Peninsula will begin, the base from which the greatest army of Islam will march forth," said Awlaki, a cleric of Yemeni descent, speaking in English. Awlaki was implicated in a failed attempt by al Qaeda in the Arabian Peninsula to bomb a US-bound airliner in 2009, and he had contacts with an American army psychiatrist who killed 13 people at a US military base the same year.

The video included a message to the American people issued by Awlaki in March 2010. But the SITE monitoring service, which tracks jihadist statements, said Awlaki’s call to join al Qaeda abroad had not appeared on that tape, although it has since been referred to in an online magazine of al Qaeda's Yemeni wing. The video also includes footage of a mysterious English speaker in what could be the debut of a new spokesman to replace Anwar al-Awlaki. The mystery man, Abu Yazeed, appears twice in the video. He is in shadow, peering off camera, and is wearing glasses and has a full beard. He is wearing what appears to be a black-and-white turban. He is identified as "Brother: Abu Yazeed."

In the video, Abu Yazeed speaks with an accent. He criticizes the United States for targeting Muslims as it fights terrorism, referencing the killings of al-Awlaki and American Samir Khan, who was killed in the same strike, and al-Awlaki’s son, who was killed in a separate strike. "Their willingness to exceed all limits is just unthinkable and by assassinating three of its own citizens far away from combat zones and with no judicial process," he says. In his second appearance, he eulogizes Samir Khan, the editor of AQAP's Inspire magazine, a publication aimed to appeal to Westerners.

A counterterrorism expert told CNN that Abu Yazeed is probably just a partial name, making it difficult to ascertain his identity. Abu Yazeed (also spelled Yazid) is a common name. The appearance of Abu Yazeed could be significant. The killings of al-Awlaki and Khan were considered a major blow to the terror group’s efforts to appeal to Westerners. "This is the first time an English speaker has appeared in an AQAP video other than al-Awlaki and is likely to mark his addition to the face of AQAP," said an analyst at the company IntelCenter, who analyzes terrorist communications. He said that Abu Yazeed could be used the way that al Qaeda in Pakistan uses Adam Gadahn: to deliver a message to Westerners.
(U) In November, New York police arrested a follower of Awlaki on suspicion of building a pipe bomb to use against US soldiers returning from Iraq and Afghanistan. Eloquent in English and Arabic, Awlaki encouraged attacks on the United States and was seen as a man who could draw in more al Qaeda recruits from Western countries. In Boston, a jury in December found a Massachusetts man guilty of supporting al Qaeda by translating Arabic messages and supporting militants travelling to Yemen for training.

(U) In Yemen, gunmen shot dead an intelligence officer in the southern province of Lahej, a security official told Reuters, adding that al Qaeda was believed to be responsible. Separately, security forces arrested seven alleged al Qaeda members who were planning attacks on government installations and officials in the south, the Defense Ministry said. The men were detained in the town of Ataq, near Abyan province, where militants linked to al Qaeda have seized swathes of territory and challenged a peace accord aimed at pulling the poor country away from civil war. The deal, brokered by Yemen's richer Gulf neighbors, aims to end a political crisis in which protests have raged for 11 months of protests against President Ali Abdullah Saleh.

(U) Top oil exporter Saudi Arabia shares US fears that more instability in Yemen could embolden al Qaeda militants there - seen by Washington as the group's most dangerous branch - in a country sitting next to oil shipping routes. Since Saleh handed over his powers to his deputy under the Gulf peace accord, a new government headed by an opposition leader has been formed. A presidential election is set to be held in February. Apart from Islamist militants, the new government is facing challenges from a southern separatist movement and a Shi'ite Muslim rebellion in the north.

(U) Analyst Comment: The death of Awlaki may increase the short-term threat that Homegrown Violent Extremists make take individual actions to conduct violent attacks in the United States. The tribute video calls on “youth” to “fight in the West.” The FBI has no information on specific, credible threats on threats in the United States, and is only noting this for situational awareness.


(U) The killing of Anwar al-Awlaki was believed to have been a major blow to the propaganda efforts of al-Qaeda’s affiliate in Yemen. But when it comes to his death’s impact on the ability of the group to carry out attacks, the picture remains as cloudy as it was when Awlaki was killed nearly four months ago. Anwar al-Awlaki was killed in a US drone strike in late September. (Associated Press)

(U) It has been more than a year since the disruption of the last known terrorist plot by al-Qaeda in the Arabian Peninsula, an attempt to bring down two cargo jets over the United States with package bombs. It has more than two years since Umar Farouk Abdulmutallab, reportedly trained by AQAP, attempted to bomb a Detroit-bound airliner. What’s more, AQAP has been most active recently advancing its regional ambitions, not threatening attacks on US soil. Still, there are at least three key reasons to remain concerned about the persistent threat posed by AQAP, according to John McLaughlin, who was deputy CIA director from 2000 to 2004 and, briefly, the agency’s acting director. The reasons, in short: speed, simplicity and strategy.

(U) “Their operation that sent Abdulmutallab here in December of 2009 was something -- it was a pick-up game. It took about a month to get that thing going,” McLaughlin said Tuesday during an event on homeland security at the Woodrow Wilson Center. “They’re cheap: The package-bomb operation, by their own estimate, cost them about $4,200. And they have a strategy, which is a thousand cuts. So, basically, attack us where they can.” There are also growing worries that AQAP is providing fighters and weaponry to other al-Qaeda affiliates, particularly al-Shabab in Somalia. Awlaki’s death has done little to
allay those concerns, terrorism experts say, even though al-Shabab is still mainly regarded as a regional threat.

(U) US officials may have branded Awlaki as AQAP’s “chief of external operations” after his death. But McLaughlin said his loss has not “had a big impact on them operationally.” The impact on AQAP’s propaganda efforts might be easier to measure. No one from AQAP’s ranks has been able to replace Awlaki as a messenger for the group. The last issue of the group’s online magazine, Inspire – believed to be largely the product of Samir Khan, the American killed alongside Awlaki in the US drone strike – came out in September. “I’m not sure how much AQAP will continue to be interested in a glitzy English-language Web journal,” Bruce Riedel, a former CIA analyst and terrorism expert, told The Post back in October. “But it’s still going to be interested in attacking the United States.”


(U) Algerian authorities have foiled a plot by an al Qaeda affiliate to ram US or European ships in the Mediterranean with an explosive-laden boat, according to an Algerian report. Three members of an alleged terror cell were arrested in connection with the plot, which Algerian authorities believe to have been directed by an al Qaeda affiliate in Algeria, al Qaeda in the Islamic Maghreb (AQIM), the Algerian daily newspaper Echorouk reported. American officials told ABC News the US government had been aware of the plot before the media report, but said Algerian authorities deserve credit for the arrests. Another official said there had not been specific reference to US ships in relation to the threat.

(U) The boat-borne suicide bomb tactic appears strikingly similar to that employed when terrorists bombed the USS Cole in October 2000. In that case, two men on a small boat laden with explosives rammed the Cole while it was refueling in Yemen, blasting a 40 ft. by 60 ft. hole in its side and killing 17 American sailors, according to the US Navy. Al Qaeda was responsible for that attack, the US government said.

(U) Though the American officials said the new plot appeared to be "in the early stages," Echorouk noted the men had already purchased a boat to be used in the bombing. The suspects reportedly confessed to the plot after their arrest. The men came to the attention of authorities after frequenting internet cafes where they surfed jihadist websites, used false names and exhibited "strange behavior," earning them the attention of "electronic crime authorities," Echorouk reported.

(U) The US officials declined to comment on any role the American government may have played in uncovering the plot, but one counter-terrorism official told ABC News, "We know that al Qaeda and their sympathizers continue to plot against the United States and our allies [and] as such, we are in touch with a number of foreign governments on issues pertaining to counter-terrorism.

(U) Azerbaijan Arrests Plot Suspects, Cites Iran link (Reuters, 25 JAN 2012)

(U) Authorities in Azerbaijan, a former Soviet republic bordering Iran, have arrested two men suspected of plotting to attack prominent foreigners including Israel's ambassador and a local rabbi, officials and media reported in January. The Azerbaijan National Security Ministry said the men were connected to an Iranian citizen who had links with Iran's intelligence. Azerbaijan, a secular Muslim country, is home to more than 9,000 Jews and has friendly ties with Israel and the United States. A major energy producer, it exports oil to Israel and imports weapons and military hardware. "Citizens of Azerbaijan - Rasim Aliyev and Ali Huseynov - were preparing an attack on public figures, who are foreign citizens," the National Security Ministry said in a statement.
(U) The US embassy issued a warning to its citizens saying "the possibility remains for actions against United States or other high-profile foreign interests in Azerbaijan". The announcement came after several state websites in Azerbaijan were rendered inaccessible for hours this month by hackers who left threats and anti-Israel messages. That incident coincided with similar cyber attacks in Israel. The ministry said the Iranian citizen, identified as Balagardash Dadashev, had helped the two buy weapons including sniper rifles, handguns and explosive devices in Iran and smuggle them to Azerbaijan. Azeri media reported the suspects had been due to receive $150,000 and their targets included the Israeli ambassador and a local rabbi. The Israeli embassy said it was "operating as usual" and declined further comment.

(U) On Jan. 16, hackers calling themselves the Azerian Cyber Army posted images of the devil over photographs of the Azeri and Israeli presidents, as well as messages saying "Servants of Jews" and "Enemies of Islam." The same day, hackers disrupted online access to the Tel Aviv Stock Exchange, El Al Airlines and 3 banks in what the government described as a cyber attack against Israel. Azeri authorities have said they had thwarted a plan by agents of Iran and Hezbollah to set off a car bomb near the Israeli embassy in Baku four years ago, as well as an alleged plot targeting the US and British embassies in 2007.

(U) In what may have been a reference to the plot, Israel's military chief said "we are witnesses to the ongoing attempts by Hezbollah and other hostile entities to execute vicious terror attacks at locations far away from the state of Israel." Earlier, police in Thailand detained a Lebanese man earlier this month on suspicion of planning an attack. Officials said he had links with Hezbollah, a Shi'ite Islamist group in Lebanon backed by Syria and Iran that is on the US blacklist of foreign terrorist organizations. Diplomatic ties between Azerbaijan and Iran are cool, but Iranian companies operate and have stakes in oil contracts in the Caspian Sea state, which exports around 1 million barrels of crude a day (bpd) westward through a pipeline operated by a consortium led by BP.

(U) Analyst Comment: The arrest in Azerbaijan of individuals possibly connected to Iranian intelligence for plotting violent attacks, and cyber attacks against Azeri and Israeli targets, indicate the increased tensions with Iran could increase the threat from Iran. In the United States, authorities have disrupted a plot to assassinate the Saudi Ambassador to the United States, and in March, 2011, hackers claiming to be from the “Iranian Cyber Army” defaced the website of the Voice of America.

(U) This bulletin has been prepared by the Tampa Division of the FBI.

(U) If you are a security officer, foreign sales representative, or employee of a business or company in Florida, you may receive unsolicited, suspicious emails from a foreign company or individual asking specific and detailed questions about your products, or inquires about starting a joint-venture or other commercial relationship. Your company or agency may also host foreign visitors or delegations that ask specific questions about or seeks access to technology or information outside the scope of their visit. If you have incidents like these to report, please contact FBI Strategic Partnership Coordinator, Patrick Laflin at 813-253-1029. Please note, cleared defense contractors are required under the NISPOM to submit suspicious contact reports to their Defense Security Service (DSS) representative.
The CI Strategic Partnership Newsletter is a product of the FBI’s Counterintelligence Program Coordination Section which plays a key role in protecting our sensitive technologies from our adversaries.

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

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

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

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

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

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

“Betrayed” represents a scenario where an FBI Intelligence Analyst is slowly but steadily compromised by a series of steps that ultimately fully compromise him into working on behalf of a foreign intelligence service. The video clearly demonstrates the traits and activities demonstrated by individuals who are involved in stealing classified information (or even proprietary information and trade secrets). The video also shows the passivity of co-workers who have clearly seen demonstrations of suspicious activity by the Intelligence Analyst, and how their failure to report the suspicious activity exasperates the situation.

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