



FBI COUNTERINTELLIGENCE STRATEGIC PARTNERSHIP NEWSLETTER



January 2012

A message from Tom Weldon:

Happy New Year to you, our valued friends and colleagues.

Although another year has come and gone, the charge to be ever vigilant never grows old, as we hope our latest newsletter illustrates. Our sincere thanks for your efforts and partnership in 2011, and the hope for even stronger ties in 2012. Again, we are here to serve you, so please do not hesitate throughout the next year to call on us at any time.

With warm regards,

Tom

Inside this issue:

FBI CI National Strategy	1
NCIX Releases Report	1
FBI Releases "Ghost Stories" Documents	2
Man Pleads Guilty to Economic Espionage	3
Fraud Conspiracy Involving Bomb Parts	4
Two Men Charged in Assassination Plot	6
Man Conceals Funding from Pakistani Gov't	7
Sophisticated Internet Fraud Scheme	8
Man Accused of Spying for Syria	10
New FBI Brochures	11
Chemist Charged with Theft of Trade Secrets	11

FBI Counterintelligence National Strategy: A Blueprint for Protecting U.S. Secrets

Espionage may seem like a throwback to earlier days of world wars and cold wars, but the threat is real and as serious as ever.

We see it—and work hard to counter it—all the time. It's not just the more traditional spies passing U.S. secrets to foreign governments, either to fatten their own wallets or to advance their ideological agendas. It's also students and scientists and plenty of others stealing the valuable trade secrets of American universities and businesses—the ingenuity that drives our economy—and providing them to other countries. It's nefarious actors sending controlled technologies overseas that help build bombs and weapons of

mass destruction designed to hurt and kill Americans and others.

In late October, in fact, we took part in a multi-agency and multi-national operation that led to the indictment of five citizens of Singapore and four of their companies for illegally exporting thousands of radio frequency modules from the U.S. Allegedly, at least 16 of these modules were later found in unexploded improvised explosive devices in Iraq. (See story on page 4.)

As the lead agency for exposing, preventing, and investigating intelligence activities on U.S. soil, the FBI continues to work to



Russian spy swaps information in a "brush pass" with an official from the Russian Mission in New York in 2004

combat these threats using our full suite of investigative and intelligence capabilities. We've mapped out our blueprint in what we call our Counterintelligence National Strategy, which is regularly updated to focus resources on the most serious current and emerging threats.

The strategy itself is classified, but we can tell

The Office of the National Counterintelligence Executive Releases Report

The report is titled, "Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011."

It was released in October and is available at: www.ncix.gov.



FBI Counterintelligence National Strategy

Continued from page 1

you what its overall goals are:

- **Keep weapons of mass destruction, advanced conventional weapons, and related technology from falling into the wrong hands**—using intelligence to drive our investigative efforts to keep threats from becoming reality. Our new Counterproliferation Center will play a major role here.
- **Protect the secrets of the U.S. intelligence community**—again, using intelligence to focus our investigative efforts and collaborating with our government partners to reduce the risk of espionage and insider threats.
- **Protect the nation’s critical assets**—like our advanced technologies and sensitive information in the defense, intelligence, economic, financial, public health, and science and technology sectors. We work to identify the source and significance of the threats against these assets, and to help their “owners” to minimize vulnerabilities.

- **Counter the activities of foreign spies**—whether they are representatives of foreign intelligence agencies or governments or are acting on their behalf, they all want the same thing: to steal U.S. secrets. Through proactive investigations, we identify who they are and stop what they’re doing.

One important aspect of our counterintelligence strategy involves strategic partnerships. And on that front, we focus on three specific areas:

- The sharing of expertise and resources of the FBI, the U.S. intelligence community, other U.S. government agencies, and global partners to combat foreign intelligence activities;
- Coordination of U.S. intelligence community efforts to combat insider threats among its own ranks; and



- Partnerships with businesses and colleges and universities to strengthen information sharing and counterintelligence awareness.

Focus on cyber activities.

Another key element of our counterintelligence strategy, according to FBI Counterintelligence Assistant Director Frank Figliuzzi, is its emphasis on detecting and deterring foreign-sponsored cyber intelligence threats to government and private sector information systems. “Sometimes,” he said, “the bad guys don’t have to physically be in the U.S. to steal targeted information...sometimes they can be halfway around the world, sitting at a keyboard.”

The FBI’s Counterintelligence National Strategy supports both the President’s National Security Strategy and the National Counterintelligence Strategy of the United States.

FBI Releases “Operation Ghost Stories” Documents & Photos

The arrests of 10 Russian spies last year provided a chilling reminder that espionage on U.S. soil did not disappear when the Cold War ended. The highly publicized case also offered a rare glimpse into the sensitive world of counterintelligence and the FBI’s efforts to safeguard the nation from those who would steal our vital secrets. Our case against the Russian Foreign Intelligence Service (SVR) operatives—dubbed Operation Ghost Stories—went on for more than a decade.

The deep-cover Russian

spies may not have achieved their objective, but they were not idle. They collected information and transmitted it back to Russia, and they were actively engaged in what is known in the spy business as “spotting and assessing.”



They identified colleagues, friends, and others who might be vulnerable targets, and it is possible they were seeking to co-opt people they encountered in the academic environment who might one day hold positions of power and influence.

Although the SVR “illegals,” as they were called, never got their hands on any classified documents, their intent from the start was serious, well-funded by the SVR, and far-ranging.

After years of gathering intelligence and making sure we knew who all the players were, we arrested the illegals on June 27, 2010. Weeks later, they pled guilty in federal court to conspiring to serve as unlawful agents of the Russian Federation within the U.S.

The released documents, photos, and videos may be seen at: http://www.fbi.gov/news/stories/2011/october/russian_103111/russian_103111

Chinese National Pleads Guilty To Economic Espionage and Theft of Trade Secrets

US Department of Justice Press Release—October 18, 2011



Kexue Huang, a Chinese national and a former resident of Carmel, Ind., pleaded guilty today to one count of economic espionage to benefit a component of the Chinese government and one count of theft of trade secrets.

This is the first trade secret prosecution in Indiana under a provision of the Economic Espionage Act that prohibits trade secret theft intended to benefit a component of a foreign government. Since its enactment in 1996, there have been a total of eight such cases charged nationwide under the Economic Espionage Act.

Huang, 48, pleaded guilty to the charges before U.S. District Judge William T. Lawrence in the Southern District of Indiana. In July 2010, Huang was charged in an indictment filed in the Southern District of Indiana for misappropriating and transporting trade secrets to the People's Republic of China (PRC) while working as a research scientist at Dow AgroSciences LLC. Today, a separate indictment filed in the District of Minnesota was unsealed, charging Huang with 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.

As a Dow employee, Huang signed an agreement that outlined his obligations in handling confidential information, including trade secrets, and 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 instrumentalities of 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.

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.

According to the plea agreement, the aggregated loss from Huang's criminal conduct exceeds \$7 million but is less than \$20 million.

"Mr. Huang used his insider status at two of America's largest agricultural companies to steal valuable trade secrets for use in his native China," said Assistant Attorney General Breuer. "We cannot allow U.S. citizens or foreign nationals to hand sensitive business information over to competitors in other countries, and we will continue our vigorous criminal enforcement of economic espionage and trade secret laws. These crimes present a danger to the U.S. economy and jeopardize our nation's leadership in innovation."

On 21 December 2011, Huang was sentenced to 87 months in prison and three years of supervised release.

The aggregated loss from Huang's criminal conduct is between \$7 million and \$20 million.

Five Individuals Indicted in a Fraud Conspiracy Involving Exports to Iran of U.S. Components Later Found in Bombs in Iraq

US Department of Justice Press Release—October 25, 2011

Indictment Also Alleges Fraud Conspiracy Involving Illegal Exports of Military Antennas to Singapore and Hong Kong

Five individuals and four of their companies have been indicted as part of a conspiracy to defraud the United States that allegedly caused thousands of radio frequency modules to be illegally exported from the United States to Iran, at least 16 of which were later found in unexploded improvised explosive devices (IEDs) in Iraq. Some of the defendants are also charged in a fraud conspiracy involving exports of military antennas to Singapore and Hong Kong.

Yesterday, authorities in Singapore arrested Wong Yuh Lan (Wong), Lim Yong Nam (Nam), Lim Kow Seng (Seng), and Hia Soo Gan Benson (Hia), all citizens of Singapore, in connection with a U.S. request for extradition. The United States is seeking their extradition to stand trial in the District of Columbia. The remaining individual defendant, Hossein Larijani, is a citizen and resident of Iran who remains at large.

The Charges

The indictment, which was returned in the District of Columbia on Sept. 15, 2010, and unsealed today, includes charges of conspiracy to defraud the United States, smuggling, illegal export of goods from the United States to Iran, illegal export of defense articles from the United States, false statements and obstruction of justice.

The charged defendants are Iranian

national Larijani, 47, and his companies Paya Electronics Complex, based in Iran, and Opto Electronics Pte, Ltd., based in Singapore. Also charged is Wong, 39, an agent of Opto Electronics who was allegedly supervised by Larijani from Iran. The indictment also charges NEL Electronics Pte. Ltd., a company in Singapore, along with NEL's owner and director, Nam, 37. Finally, the indictment charges Corezing International Pte. Ltd., a company in Singapore that maintained offices in China, as well as Seng, 42, an agent of Corezing, and Hia, 44, a manager, director and agent of Corezing.

Wong, Nam, Seng and Hia allegedly conspired to defraud the United States by impeding U.S. export controls relating to the shipment of 6,000 radio frequency modules from a Minnesota company through Singapore to Iran, some of which were later found in unexploded IEDs in Iraq. Seng and Hia are also accused of conspiring to defraud the United States relating to the shipment of military antennas from a Massachusetts company to Singapore and Hong Kong. Singapore has agreed to seek extradition for Wong and Nam on the charge of conspiracy to defraud the United States relating to the components shipped to Iran, and to seek extradition for Seng and Hia on the charge of conspiracy to defraud the United States relating to the military antenna exports.

In coordination with the criminal actions announced today, the Commerce Department announced the addition of 15 persons located in China, Hong Kong, Iran and



Singapore to the Commerce Department's Entity List. In addition to the five individual defendants in this case, the Commerce Department named additional companies and individuals associated with this conspiracy. In placing these parties on the Entity List, the Commerce Department is imposing a licensing requirement for any item subject to Commerce regulation with a presumption that such a license would be denied.

Exports of U.S. Components Later Found in IEDs

According to the indictment, IEDs caused roughly 60 percent of all American combat casualties in Iraq between 2001 and 2007. The first conspiracy alleged in the indictment involved radio frequency modules that have several commercial applications, including in wireless local area networks connecting printers and computers in office settings. These modules include encryption capabilities and have a range allowing them to transmit data wirelessly as far as 40 miles when configured with a high-gain antenna. These same modules also have potentially lethal applications. Notably, during 2008 and 2009, coalition forces in Iraq recovered numerous modules made by the Minnesota firm that had been utilized as part of the remote detonation system for IEDs.

The indictment alleges that, between June 2007 and February 2008, the defendants fraudulently purchased and caused 6,000 modules to be illegally exported from the Minnesota company

Five Individuals Indicted in a Fraud Conspiracy

Continued from page 4

through Singapore, and later to Iran, in five shipments, knowing that the export of U.S.-origin goods to Iran was a violation of U.S. law. In each transaction, the defendants allegedly told the Minnesota firm that Singapore was the final destination of the goods. The defendants also caused false documents to be filed with the U.S. government, in which they claimed that a telecommunications project in Singapore was the final end-use for the modules. In reality, each of the five shipments was routed from Singapore to Iran via air cargo. The alleged recipient of all 6,000 modules in Iran was Larijani, who had directed Wong, his employee in Singapore, to order them.

According to the indictment, the defendants profited considerably from their illegal trade. The defendants allegedly made tens of thousands of dollars for arranging these illegal exports from the United States through Singapore to Iran.

The indictment alleges that several of the 6,000 modules the defendants routed from Minnesota to Iran were later discovered by coalition forces in Iraq, where they were being used as part of the remote detonation systems of IEDs. In May 2008, December 2008, April 2009, and July 2010, coalition forces found no less than 16 of these modules in unexploded IEDs recovered in Iraq, the indictment alleges.

During this period, some of the defendants were allegedly communicating with one another about U.S. laws prohibiting the export of U.S.-origin goods to Iran. For example, between October 2007 and June 2009, Nam contacted Larijani in Iran at least six times and discussed the Iran prohibitions

and U.S. prosecutions for violation of these laws. Nam later told U.S. authorities that he had never participated in illicit exports to Iran, even though he had participated in five such shipments, according to the indictment.

Exports of Military Antennas

The indictment further charges Seng, Hia, and Corezing with a separate fraud conspiracy involving the illegal export of two types of military antenna from the United States. The indictment alleges that these defendants conspired to defraud the United States by causing a total of 55 cavity-backed spiral antennas and biconical antennas to be illegally exported from a Massachusetts company to Singapore and Hong Kong without the required State Department license.

These military antennas are controlled for export as U.S. munitions and are used in airborne and shipboard environments. The indictment states that the biconical antenna, for example, is used in military aircraft such as the F-4 Phantom, the F-15, the F-111, the A-10 Thunderbolt II and the F-16 combat jets.

Seng, Hia and Corezing are alleged to have, among other things, conspired to undervalue the antennas to circumvent U.S. regulations on the filing of shipper's export declarations to the U.S. government. They also allegedly used false names and front companies to obtain the antennas illegally from the United States.

Additional Misrepresentations

The indictment further alleges that Larijani, based in Iran, made false statements about doing business with an accused Iranian

procurement agent and that he attempted to obstruct an official proceeding by the U.S. Department of Commerce.

In January 2010, the Department of Commerce placed Larijani's company, Opto Electronics, on the Entity List, which is a list of companies to which U.S. businesses cannot export controlled dual-use items without obtaining U.S. government licenses. In response, Larijani repeatedly contacted Commerce Department officials in Washington, D.C., from Iran, requesting that his company be removed from the Entity List, according to the indictment. Commerce officials advised Larijani that, in considering whether his firm should be removed from the list, he needed to disclose whether he or his firm had any involvement with Majid Kakavand or Evertop Services Sdn Bhd.

Kakavand is an accused Iranian procurement agent who has been indicted in the United States, along with his Malaysian company Evertop Services, for illegally exporting U.S. goods to Iran, including to military entities in Iran involved in that nation's nuclear and ballistic missile programs. Kakavand remains a fugitive and is believed to be in Iran.

According to the indictment, Larijani denied to Commerce officials on three occasions that he or his company, Opto Electronics, had done any business with Kakavand or Evertop Services. In fact, the indictment alleges that Larijani had been in communication with others about his business dealings with Kakavand on at least five occasions from 2006 through 2009.

Two Men Charged in Alleged Plot to Assassinate Saudi Arabian Ambassador to the United States

US Department of Justice Press Release—October 11, 2011

Two individuals have been charged in New York for their alleged participation in a plot directed by elements of the Iranian government to murder the Saudi Ambassador to the United States with explosives while the Ambassador was in the United States.

A criminal complaint filed today in the Southern District of New York charges Manssor Arbabsiar, a 56-year-old naturalized U.S. citizen holding both Iranian and U.S. passports, and Gholam Shakuri, an Iran-based member of Iran's Qods Force, which is a special operations unit of the Iranian Islamic Revolutionary Guard Corps (IRGC) that is said to sponsor and promote terrorist activities abroad.

Both defendants are charged with conspiracy to murder a foreign official; conspiracy to engage in foreign travel and use of interstate and foreign commerce facilities in the commission of murder-for-hire; conspiracy to use a weapon of mass destruction (explosives); and conspiracy to commit an act of international terrorism transcending national boundaries. Arbabsiar is further charged with an additional count of foreign travel and use of interstate and foreign commerce facilities in the commission of murder-for-hire.

Shakuri remains at large. Arbabsiar was arrested on Sept. 29, 2011, at New York's John F. Kennedy International Airport and will make his initial appearance today before in federal court in Manhattan. He faces a maximum potential sentence of life in prison if convicted of all the charges.

The Alleged Plot

The criminal complaint alleges that, from the spring of 2011 to October 2011, Arbabsiar and his Iran-based co-conspirators, including Shakuri of the Qods Force, have been plotting

the murder of the Saudi Ambassador to the United States. In furtherance of this conspiracy, Arbabsiar allegedly met on a number of occasions in Mexico with a DEA confidential source (CS-1) who has posed as an associate of a violent international drug trafficking cartel. According to the complaint, Arbabsiar arranged to hire CS-1 and CS-1's purported accomplices to murder the Ambassador, and Shakuri and other Iran-based co-conspirators were aware of and approved the plan. With Shakuri's approval, Arbabsiar has allegedly caused approximately \$100,000 to be wired into a bank account in the United States as a down payment to CS-1 for the anticipated killing of the Ambassador, which was to take place in the United States.

According to the criminal complaint, the IRGC is an arm of the Iranian military that is composed of a number of branches, one of which is the Qods Force. The Qods Force conducts sensitive covert operations abroad, including terrorist attacks, assassinations and kidnappings, and is believed to sponsor attacks against Coalition Forces in Iraq. In October 2007, the U.S. Treasury Department designated the Qods Force for providing material support to the Taliban and other terrorist organizations.

The complaint alleges that Arbabsiar met with CS-1 in Mexico on May 24, 2011, where Arbabsiar inquired as to CS-1's knowledge with respect to explosives and explained that he was interested in, among other things, attacking an embassy of Saudi Arabia. In response, CS-1 allegedly indicated that he was knowledgeable with respect to C-4 explosives. In June and July 2011, the complaint alleges, Arbabsiar returned to Mexico and held additional meetings with CS-1, where Arbabsiar explained that his



associates in Iran had discussed a number of violent missions for CS-1 and his associates to perform, including the murder of the Ambassador.

\$1.5 Million Fee for Alleged Assassination

In a July 14, 2011, meeting in Mexico, CS-1 allegedly told Arbabsiar that he would need to use four men to carry out the Ambassador's murder and that his price for carrying out the murder was \$1.5 million. Arbabsiar allegedly agreed and stated that the murder of the Ambassador should be handled first, before the execution of other attacks. Arbabsiar also allegedly indicated he and his associates had \$100,000 in Iran to pay CS-1 as a first payment toward the assassination and discussed the manner in which that payment would be made.

During the same meeting, Arbabsiar allegedly described to CS-1 his cousin in Iran, who he said had requested that Arbabsiar find someone to carry out the Ambassador's assassination. According to the complaint, Arbabsiar indicated that his cousin was a "big general" in the Iranian military; that he focuses on matters outside Iran and that he had taken certain unspecified actions related to a bombing in Iraq.

In a July 17, 2011, meeting in Mexico, CS-1 noted to Arbabsiar that one of his workers had already traveled to Washington, D.C., to surveil the Ambassador. CS-1 also raised the possibility of innocent bystander casualties. The complaint alleges that Arbabsiar made it clear that the assassination needed to go forward, despite mass casualties, telling CS-1, "They want that guy [the Ambassador] done [killed], if the

Alleged Plot to Assassinate Saudi Arabian Ambassador

Continued from page 6

hundred go with him f**k 'em." CS-1 and Arbabsiar allegedly discussed bombing a restaurant in the United States that the Ambassador frequented. When CS-1 noted that others could be killed in the attack, including U.S. senators who dine at the restaurant, Arbabsiar allegedly dismissed these concerns as "no big deal."

On Aug. 1, and Aug. 9, 2011, with Shakuri's approval, Arbabsiar allegedly caused two overseas wire transfers totaling approximately \$100,000 to be sent to an FBI undercover account as a down payment for CS-1 to carry out the assassination. Later, Arbabsiar allegedly explained to CS-1 that he would provide the remainder of the \$1.5 million after the assassination. On Sept. 20, 2011, CS-1 allegedly told Arbabsiar that the operation was ready and requested that Arbabsiar either pay one half of the agreed upon price (\$1.5 million) for the murder or that Arbabsiar personally travel to Mexico as collateral for the final payment of the fee. According to the complaint,

Arbabsiar agreed to travel to Mexico to guarantee final payment for the murder.

Arrest and Alleged Confession

On or about Sept. 28, 2011, Arbabsiar flew to Mexico. Arbabsiar was refused entry into Mexico by Mexican authorities and, according to Mexican law and international agreements; he was placed on a return flight destined for his last point of departure. On Sept. 29, 2011, Arbabsiar was arrested by federal agents during a flight layover at JFK International Airport in New York. Several hours after his arrest, Arbabsiar was advised of his *Miranda* rights and he agreed to waive those rights and speak with law enforcement agents. During a series of *Mirandized* interviews, Arbabsiar allegedly confessed to his participation in the murder plot.

According to the complaint, Arbabsiar also admitted to agents that, in connection with this plot, he was recruited, funded and directed by men he understood to be senior officials in Iran's Qods Force. He

allegedly said these Iranian officials were aware of and approved of the use of CS-1 in connection with the plot; as well as payments to CS-1; the means by which the Ambassador would be killed in the United States and the casualties that would likely result.

Arbabsiar allegedly told agents that his cousin, who he had long understood to be a senior member of the Qods Force, had approached him in the early spring of 2011 about recruiting narco-traffickers to kidnap the Ambassador. Arbabsiar told agents that he then met with the CS-1 in Mexico and discussed assassinating the Ambassador. According to the complaint, Arbabsiar said that, afterwards, he met several times in Iran with Shakuri and another senior Qods Force official, where he explained that the plan was to blow up a restaurant in the United States frequented by the Ambassador and that numerous bystanders could be killed, according to the complaint. The plan was allegedly approved by these officials.

Virginia Man Pleads Guilty in Scheme to Conceal Pakistan Government Funding for His U.S. Lobbying Efforts

US Department of Justice Press Release—December 7, 2011

Syed Ghulam Nabi Fai, 62, a U.S. citizen and resident of Fairfax, Va., pleaded guilty today to conspiracy and tax violations in connection with a decades-long scheme to conceal the transfer of at least \$3.5 million from the government of Pakistan to fund his lobbying efforts in America related to Kashmir.

Fai faces a maximum potential sentence of five years in prison for the conspiracy count and a maximum three years in prison for the tax violation. Judge O'Grady set sentencing for March 9, 2012. As part of his plea agreement, Fai has agreed to forfeit his interest in

\$142,851.32 seized by the government in July 2011.

Fai served as the director of the Kashmiri American Council (KAC), a non-governmental organization in Washington, D.C., that held itself out to be run by Kashmiris, financed by Americans and dedicated to raising the level of knowledge in the United States about the struggle of the Kashmiri people for self-determination. But according to court documents, the KAC was secretly funded by officials employed by the government of Pakistan, including the Inter-Services Intelligence Directorate (ISI).

Today, Fai admitted that, from 1990 until about July 18, 2011, he conspired with others to obtain money from officials employed by the government of Pakistan, including the ISI, for the operation of the KAC in the United States, and that he did so outside the knowledge of the U.S. government and without attracting the attention of law enforcement and regulatory authorities.

To prevent the Justice Department, FBI, Department of Treasury and the IRS from learning the source of the money he received from officials employed by the government of



Scheme to Conceal Pakistan Government Funding

Continued from page 7

Pakistan and the ISI, Fai made a series of false statements and representations, according to court documents. For example, Fai told FBI agents in March 2007 that he had never met anyone who identified himself as being affiliated with the ISI and, in May 2009, he falsely denied to the IRS on a tax return for the KAC that the KAC had received any money from foreign sources in 2008.

In addition, according to court documents, Fai sent a letter in April 2010 to the Justice Department falsely asserting that the KAC was not funded by the government of Pakistan. Later that year, Fai falsely denied to the IRS that the KAC had received any money from foreign sources in 2009. In July 2011, Fai falsely denied to FBI agents that he or the KAC received money from the ISI

or government of Pakistan.

In fact, Fai repeatedly submitted annual KAC strategy reports and budgetary requirements to Pakistani government officials for approval. For instance, in 2009, Fai sent the ISI a document entitled "Plan of Action of KAC / Kashmir Centre, Washington, D.C., for the Fiscal Year 2010," which itemized KAC's 2010 budget request of \$658,000 and listed Fai's plans to secure U.S. congressional support for U.S. action in support of Kashmiri self-determination.

Fai also admitted that, from 1990 until about July 18, 2011, he corruptly endeavored to obstruct and impede the due administration of the internal revenue laws by arranging for the transfer of at least \$3.5 million to the KAC from employees of the government of Pakistan and the ISI.

According to court documents, Fai accepted the transfer of such money to the KAC from the ISI and the government of Pakistan through his co-defendant Zaheer Ahmad and middlemen (straw donors), who received reimbursement from Ahmad for their purported "donations" to the KAC. Fai provided letters from the KAC to the straw donors documenting that their purported "donations" to the KAC were tax deductible and encouraged these donors to deduct the transfers as "charitable" deductions on their personal tax returns. Fai concealed from the IRS that the straw donors' purported KAC "donations" were reimbursed by Ahmad, using funds received from officials employed by the ISI and the government of Pakistan.

Seven Individuals Charged for Engineering Sophisticated Internet Fraud Scheme That Infected Millions of Computers Worldwide and Manipulated Internet Advertising Business

US Department of Justice Press Release—November 9, 2011

Malware Secretly Re-Routed More Than 4 Million Computers, Generating at Least \$14 Million in Fraudulent Advertising Fees for the Defendants

Charges were announced against six Estonian nationals and one Russian national for engaging in a massive and sophisticated Internet fraud scheme that infected with malware more than four million computers located in over 100 countries. Of the computers infected with malware, at least 500,000 were in the United States, including computers belonging to U.S. government agencies, such as NASA; educational institutions; non-profit organizations; commercial

businesses; and individuals. The malware secretly altered the settings on infected computers enabling the defendants to digitally hijack Internet searches and re-route computers to certain websites and advertisements, which entitled the defendants to be paid. The defendants subsequently received fees each time these websites or ads were clicked on or viewed by users.

Six of the defendants, Vladimir Tsastsin, 31, Timur Gerassimenko, 31, Dmitri Jegorov, 33, Valeri Aleksejev, 31, Konstantin Poltev, 28, and Anton Ivanov, 26, all Estonian nationals, were arrested and taken into custody yesterday in Estonia by the Estonian Police and Border Guard Board. The U.S.

Attorney's Office will seek their extradition to the United States. The seventh defendant, Andrey Taame, 31, a Russian national, remains at large.

The Cyber-Fraud Scheme

As alleged in the Indictment, from 2007 until October 2011, the defendants controlled and operated various companies that masqueraded as legitimate publisher networks (the "Publisher Networks") in the Internet advertising industry. The Publisher Networks entered into agreements with ad brokers under which they were paid based on the number of times that Internet users clicked on the links for certain websites or advertisements, or based on the

Sophisticated Internet Fraud Scheme

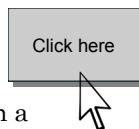
Continued from page 8

number of times that certain advertisements were displayed on certain websites. Thus, the more traffic to the advertisers' websites and display ads, the more money the defendants earned under their agreements with the ad brokers. As alleged in the Indictment, the defendants fraudulently increased the traffic to the websites and advertisements that would earn them money. They accomplished this by making it appear to advertisers that the Internet traffic came from legitimate clicks and ad displays on the defendants' Publisher Networks when, in actuality, it had not.

To carry out the scheme, the defendants and their co-conspirators used what are known as "rogue" Domain Name System ("DNS") servers, and malware ("the Malware") that was designed to alter the DNS server settings on infected computers. Victims' computers became infected with the Malware when they visited certain websites or downloaded certain software to view videos online. The Malware altered the DNS server settings on victims' computers to route the infected computers to rogue DNS servers controlled and operated by the defendants and their co-conspirators. The re-routing took two forms that are described in detail below: "click hijacking" and "advertising replacement fraud." The Malware also prevented the infected computers from receiving anti-virus software updates or operating system updates that otherwise might have detected the Malware and stopped it. In addition, the infected computers were also left vulnerable to infections by other viruses.

Click Hijacking

When the user of an infected computer clicked on a search result link displayed



through a search engine query, the Malware caused the computer to be re-routed to a different website. Instead of being brought to the website to which the user asked to go, the user was brought to a website designated by the defendants. Each "click" triggered payment to the defendants under their advertising agreements. This click hijacking occurred for clicks on unpaid links that appear in response to a user's query as well as clicks on "sponsored" links or advertisements that appear in response to a user's query—often at the top of, or to the right of, the search results—thus causing the search engines to lose money.

Advertising Replacement Fraud

Using the DNS Changer Malware and rogue DNS servers, the defendants also replaced legitimate advertisements on websites with substituted advertisements that triggered payments to the defendants.

The defendants earned millions of dollars under their advertising agreements, not by legitimately displaying advertisements through their Publisher Networks, but rather by using the Malware to fraudulently drive Internet traffic to the websites and ads that would earn them more money.

The defendants' scheme also deprived legitimate website operators and advertisers of substantial monies and advertising revenue. In addition to search engines losing revenue as a result of click hijacking on their sponsored search result listings, advertisers lost money by paying for clicks that they believed came from interested computer users, but which were in fact fraudulently engineered by the defendants. Furthermore, the defendants' conduct risked reputational harm to businesses

that paid to advertise on the Internet—but that had no knowledge or desire for computer users to be directed to their websites or advertisements through the fraudulent means used by the defendants.

Remediation Efforts

In conjunction with the arrests yesterday, authorities in the United States seized computers at various locations, froze the defendants' financial accounts, and disabled their network of U.S.-based computers—including dozens of rogue DNS servers located in New York and Chicago. Additionally, authorities in the United States took steps with their foreign counterparts to freeze the defendants' assets located in other countries. Remediation efforts were immediately undertaken to minimize any disruption of Internet service to the users of computers infected with the Malware. This remediation was necessary because the dismantling of the defendants' rogue DNS servers—to which millions of computers worldwide had been redirected—would potentially have caused all of those computers, for all practical purposes, to lose access to websites.

The defendant's rogue DNS servers have been replaced with legitimate ones. Internet Systems Consortium ("ISC"), a not-for-profit entity, was appointed by the court to act as a third-party receiver for a limited period of 120 days during which time it will administer the replacement DNS servers. Although the replacement DNS servers will provide continuity of Internet service to victims, those replacement servers will not remove the Malware from the infected computers. Users who believe their computers may be infected can find additional information at FBI.gov.

Man Accused of Acting as Unregistered Agent of Syrian Government and Spying on Syrian Protestors in America

US Department of Justice Press Release—October 12, 2011

Mohamad Anas Haitham Soueid, 47, a resident of Leesburg, Va., has been charged for his alleged role in a conspiracy to collect video and audio recordings and other information about individuals in the United States and Syria who were protesting the government of Syria and to provide these materials to Syrian intelligence agencies in order to silence, intimidate and potentially harm the protestors.

Soueid, aka “Alex Soueid” or “Anas Alswaid,” a Syrian-born naturalized U.S. citizen, was charged by a federal grand jury on Oct. 5, 2011, in a six-count indictment in the Eastern District of Virginia. Soueid is charged with conspiring to act and acting as an agent of the Syrian government in the United States without notifying the Attorney General as required by law; two counts of providing false statements on a firearms purchase form; and two counts of providing false statements to federal law enforcement.

According to the indictment, since March 2011, Soueid has acted in the United States as an agent of the Syrian *Mukhabarat*, which refers to the intelligence agencies for the Government of Syria, including the Syrian Military Intelligence and General Intelligence Directorate. At no time while acting as an agent of the government of Syria in this country did Soueid provide prior notification to the Attorney General as required by law, the indictment alleges.

Under the direction and control of Syrian officials, Soueid is accused of recruiting individuals living in the United States to collect information on and make audio and video

recordings of protests against the Syrian regime – including recordings of conversations with individual protestors – in the United States and Syria. He is also charged with providing the recordings and other information to individuals working for the *Mukhabarat*. According to the indictment, Soueid and others conspired to use this information to undermine, silence, intimidate and potentially harm those in the United States and Syria who engaged in the protests.

The indictment states that in late June 2011, the Syrian government paid for Soueid to travel to Syria, where he met with intelligence officials and spoke with President Bashar al-Assad in private.

He returned to the United States in early July 2011, and he was searched and questioned at Dulles International Airport upon his arrival. The indictment states that Soueid communicated with his “boss,” an unindicted co-conspirator (or UCC-1) who was working for the *Mukhabarat*, soon after to alert him of the search and questioning and to assure the individual that the airport encounter would not “stop the project.”

In addition to the recordings, Soueid is accused of providing the *Mukhabarat* contact information, including phone numbers and email addresses, for protestors in the United States. In a handwritten letter sent to UCC-1, Soueid allegedly expressed his belief that violence against protestors – including raiding their homes – was justified and that any method should be used to deal with the protestors. The indictment also

alleges that Soueid provided information regarding U.S. protestors against the Syrian regime to an individual who worked at the Syrian Embassy in Washington, D.C.



On Aug. 3, 2011, FBI agents interviewed Soueid, and the indictment accuses him of lying to the agents when he denied that he had collected information on U.S. persons and transmitted that information to the government of Syria. In addition, Soueid allegedly made further false statements when he denied to FBI agents that he had directed someone to audio or videotape a conversation, meeting, rally or protest, or that he was aware of any individual taking photographs or videotaping people. He also allegedly made false statements when he denied that he had ever been an agent of the Syrian government or a foreign intelligence officer.

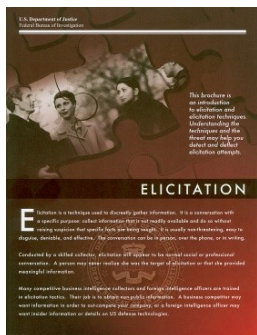
The indictment states that the day following the interview, Soueid asked UCC-1 to inform the *Mukhabarat* about his FBI interview.

In addition, the indictment alleges that, when purchasing a Beretta pistol on July 11, 2011, Soueid listed a false current residence address on a firearms purchase application and in records that were kept by a licensed firearms dealer.

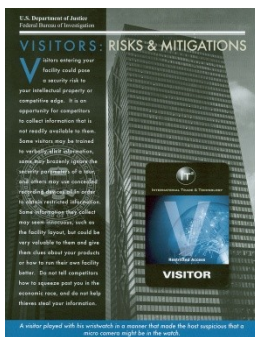
The public is reminded that an indictment contains mere allegations and that a defendant is presumed innocent unless and until proven guilty.

Introducing Two New Brochures from the FBI:

Visitors: Risks & Mitigations—a guide to protecting your intellectual property when visitors tour or enter your facility.



Elicitation—an introduction to elicitation and elicitation techniques and how to defend against them.



They are available on the FBI's website, along with additional brochures, or through your local FBI Strategic Partnership Coordinator.

The FBI Counterintelligence Strategic Partnership Program's Mission:

To work with academia, private industry and the intelligence community to foster proactive strategies to negate attempts by foreign adversaries to victimize U.S. interests.

Each of the FBI's 56 field offices has a Counterintelligence Strategic Partnership Coordinator who works locally to further this mission. For additional information, assistance, or training, contact your local FBI office's Strategic Partnership Coordinator.



www.fbi.gov/about-us/investigate/counterintelligence/strategic-partnerships

Chemical Scientist Charged with Theft of Trade Secrets

November 10, 2011

A criminal complaint was filed with the US District Court in Utah on November 10, 2011, against Prabhu Mohapatra, a Senior Scientist employed by Frontier Scientific Inc. (FSI), for theft of trade secrets.

According to the complaint, on October 25, 2011, Mohapatra's coworker observed Mohapatra create a document on his desktop computer that contained the recipe for the process of manufacturing 2,2'-dipyrrromethane, a trade secret of FSI. The coworker saw him convert the file into a PDF file, then access his personal email account. FSI management was informed and they reviewed Mohapatra's computer activity. It appeared he emailed the 2,2' dipyrromethane file to a pharmaceutical chemical company in India.

On October 26, 2011, the coworker again observed Mohapatra as he

placed the chemical recipe for Fe [III] meso-tetra [o-dichlorophenyl] porphine chloride in a Word document and PDF file. He then appeared to access his personal email account and send the file.

FSI again reviewed the computer activity of Mohapatra and noted the above email exchange, as well as a reply that told Mohapatra that information provided by Mohapatra would enable the production of five-six months worth of products for Porphyrin Systems, a direct competitor of FSI. The computer analysis also showed that Mohapatra deleted the Word and PDF files after sending them, and deleted the emails from his email account.

After being placed on administrative leave,

Mohapatra admitted he was involved in the creation of an Indian company called Medchemblox that would produce and sell the same type of products as FSI.

When Mohapatra was hired by FSI, he signed non-disclosure agreements that discussed the proprietary nature of the chemical recipes and the need to protect the recipes. In addition, Mohapatra had been previously told not to share any trade secret information with the individual in India.

Mohapatra was arrested November 14 and released the same day after appearing in federal court in Salt Lake City. He faces up to 10 years in prison and a \$250,000 fine if convicted.

