EIB World Trade Headlines

Evolutions In Business • www.eib.com • (978) 256-0438
Fax: (978) 250-4529 • P.O. Box 4008. Chelmsford. MA 01824

May 15, 2016 - Volume 8, Issue 9

CYBER, HACKING, DATA THEFT, COMPUTER INTRUSIONS & RELATED

Dropping USB Drives Is the Easiest Trick Hackers Can Use

YAHOO TECH
April 12, 2016

Hackers have devised one of the most effective and direct traps for gaining access to your most sensitive systems: simply leaving stuff on the ground. Researchers at the University of Illinois and University of Michigan found that if you discard a USB stick somewhere, there's a nearly 50% chance that someone will pick it up, plug it into a computer and start clicking around inside.
This is where it gets scary. If that drive has malicious software on it, it's all too easy for a hacker to access your computer. The threat is so well-known it was featured in a *Mr. Robot* plot. And yet humans will, without fail, disregard the risk and plug in unknown drives.

The experiment: Researchers dropped about 300 USB drives around the University of Illinois Urbana-Champaign campus. The researchers labeled them in a variety of ways, like attaching keys or a return mailing address to some of them, and filled the USB drives with fake files like "résumé" and "pictures."
It took only six minutes for someone to get one of the drives and plug it in somewhere. Out of all the dropped drives, a full 48% were picked up, plugged in and explored.
"This surprisingly high conversion rate demonstrates that USB drop attacks are a real threat and underscores the importance of educating users on the risk of

*(*Continued On The Following Page)*

NEWSLETTER NOTES

plugging in untrusted USB devices," Google researcher Elie Bursztein, who worked on the study, wrote on his blog. People were less likely to click around inside the drive when there was a label attached. Many reported back to the researchers that they really just wanted to help find the drive's owner. Otherwise, the research found that the attack was effective no matter who picked up the drive or where they were. Curiosity got the best of them.

Use protection: Hackers in movies have to use crack-shot coding skills and custom equipment to gain access to secure systems. But in real life, everyday "hacking" is mostly about taking advantage of people's gullibility. They can guess passwords, impersonate you over the phone to a customer support representative or just set up a fake public Wi-Fi network and wait for you to connect.

There are a few basic measures to protect yourself from basic exploits, like creating complicated passwords and keeping your software up to date.

But when it comes to USB drives, you could just ban them entirely — at your company, in your home, or just by instituting a no-plugging-things-in policy for yourself.

"With the advent of cloud storage and fast internet connections, this is policy is not as unreasonable as it was a few years back," Bursztein wrote.

ARRESTS, TRIALS AND CONVICTIONS U.S. Nuclear Engineer, China General Nuclear Power Company and Energy Technology International Indicted in Nuclear Power Conspiracy against the United States

Department of Justice
U.S. Attorney's Office
Eastern District of Tennessee
FOR IMMEDIATE RELEASE
Thursday, April 14, 2016

WASHINGTON – A two-count indictment was unsealed today in the Eastern District of Tennessee charging Szuhsiung Ho, aka Allen Ho, a citizen of the United States; China General Nuclear Power Company (CGNPC), formerly known as the China Guangdong Nuclear Power Company and Energy Technology International (ETI) for conspiracy to unlawfully engage and participate in the production and development of special nuclear material outside the United States, without the required authorization from the U.S. Department of Energy. This authorization is required by U.S. law and is robustly observed through frequent legal U.S.- China civil nuclear cooperation. Ho was also charged with conspiracy to act in the United States as an agent of a foreign government.

The announcement was made by Assistant Attorney General for National Security John P. Carlin, Acting U.S. Attorney Nancy

*(*Continued On The Following Column)*

Stallard Harr of the Eastern District of Tennessee and Executive Assistant Director Michael Steinbach of the FBI's National Security Branch.

Acting U.S. Attorney Harr affirmed the importance of this case by stating, "The prosecution of individuals who potentially endanger our U.S. citizens by violating laws enacted to ensure our national security, has been and will remain a priority for the U.S. Attorney's Office in eastern Tennessee."

"Allen Ho, at the direction of a Chinese state-owned nuclear power company allegedly approached and enlisted U.S. based nuclear experts to provide integral assistance in developing and producing special nuclear material in China," said Assistant Attorney General Carlin. "Ho did so without registering with the Department of Justice as an agent of a foreign nation or authorization from the U.S. Department of Energy. Prosecuting those who seek to evade U.S. law by attaining sensitive nuclear technology for foreign nations is a top priority for the National Security Division."

"The arrest and indictment in this case send an important message to the U.S. nuclear community that foreign entities want the information you possess," said Executive Assistant Director Steinbach. "The federal government has regulations in place to oversee civil nuclear cooperation, and if those authorities are circumvented, this can result in significant damage to our national security. The U.S. will use all of its law enforcement tools to stop those who try to steal U.S. nuclear technology and expertise."

According to the indictment, Ho is a nuclear engineer employed by CGNPC as a senior advisor and is also the owner and president of ETI. Born in China, he is a naturalized U.S. citizen with dual residency in Delaware and China. CGNPC, which is owned by China's State-Owned Assets Supervision and Administration Commission of the State Council, is the largest nuclear power company in China and specializes in the development and manufacture of nuclear reactors. ETI is a Delaware corporation headquartered in Ho's home in Wilmington, Delaware.

According to allegations in the indictment, which was returned on April 5, 2016, beginning in 1997 and continuing through April 2016, Ho, CGNPC and ETI allegedly conspired with others to engage and participate in the development and production of special nuclear material in China, with the intent to secure an advantage to China and without specific authorization to do so from the U.S. Secretary of Energy, as required by law. In particular, the defendants allegedly sought technical assistance related to, among other things, CGNPC's Small Modular Reactor Program; CGNPC's Advanced Fuel Assembly Program; CGNPC's Fixed In-Core Detector System; and verification and validation of nuclear reactor-related computer codes.

The indictment further alleges that Ho, under the direction of CGNPC, identified, recruited and executed contracts with U.S.-based experts from the civil nuclear industry who provided technical assistance related to the development and production of special nuclear material for CGNPC in China. Ho and CGNPC also allegedly facilitated the travel to China and

(*Continued On The Following Page)

payments to the U.S.-based experts in exchange for their services.
The indictment further alleges that during this same period of time, Ho conspired with others to knowingly act as an agent of China without prior notification to the Attorney General, as required by law. On or about Oct. 4, 2009, Ho allegedly told experts who he was attempting to recruit that, "China has the budget to spend," and that he needed assistance so that, "China will be able to design their Nuclear Instrumentation System independently and manufactur[e] them independently after the project is complete." In further correspondence with nuclear experts in the United States, Ho made clear that he was charged with obtaining necessary expertise from the United States at the direction of the CGNPC and the China Nuclear Power Technology Research Institute, a subsidiary of CGNPC, and that he was to do so surreptitiously.
If convicted, the charge of conspiracy to unlawfully engage and participate in the production and development of special nuclear material outside the United States carries a maximum sentence of life in prison and a $250,000 fine. The charge of conspiring to act in the United States as an agent of a foreign government carries a maximum sentence of 10 years in prison along with fines and supervised release.
The charges contained in the indictment are merely accusations, and the defendants are presumed innocent unless and until proven guilty.
The case is being investigated by the FBI, the Tennessee Valley Authority-Office of the Inspector General, the Department of Energy-National Nuclear Security Administration and the U.S. Immigration and Customs Enforcement, Homeland Security Investigations, with assistance from other agencies. The case is being prosecuted by Assistant U.S. Attorney Charles E. Atchley Jr. of the Eastern District of Tennessee and Trial Attorney Casey T. Arrowood of the National Security Division's Counter intelligence and Export Control Section.

Iranian Cyber Attack on New York Dam Shows Future of War

TIME.COM
March 24, 2016
The first nationstate warfare took place between soldiers on the ground, and then ships at sea. In the 20th Century, the battles moved into the skies. On Thursday, the Justice Department claimed Iran had attacked U.S. infrastructure online, by infiltrating the computerized controls of a small dam 25 miles north of New York City, heralding a new way of war on American soil.
"We can tell the world that hackers affiliated with the Iranian government attacked U.S. systems, and we seek to bring them to justice for their crimes," Assistant Attorney General John P. Carlin said, unveiling charges against seven Iranians for cyber attacks. The hackers, members of the Iran's Islamic Revolutionary Guards Corps, also targeted several financial

*(*Continued On The Following Column)*

institutions, the New York Stock Exchange and AT&T with barrages of incoming emails designed to slow or shut down some of their computers, according to the indictment.

Hackers broke into the command and control system of the dam in 2013, apparently through a cellular modem. While 34-year-old Hamid Firoozi should have been able to release water from behind the dam given his remote access, he "did not have that capability because the sluice gate had been manually disconnected for maintenance at the time of the intrusion," the U.S. government said.
While insignificant in the overall scheme—the 20-foot, flood-control dam is on Blind Brook in Rye Brook, N.Y.—it signals the desire of some foreign nations to infect, and potentially operate, U.S. infrastructure. "They were sending a shot across our bow," Senator Charles Schumer, D-N.Y., said of the Iranian probing of the dam earlier this month. "They were saying that we can damage, seriously damage, our critical infrastructure and put the lives and property of people at risk."
There is next to no chance the Iranians will end up in U.S. courts. But U.S. officials say the "name and shame" effort is designed to make clear the U.S. knows what happened, and to deter those involved from traveling overseas, where they could be arrested.
The intrusion happened as the U.S. and Iran readied to negotiate a deal curbing Tehran's nuclear-development program, and followed by two years a massive U.S.-Israeli cyber attack dubbed Stuxnet on Iran's nuclear centrifuges designed to thwart its atomic

This isn't the first time the U.S. has linked cyber attacks to foreign nations. In recent years, the U.S. government publicly accused North Korea of hacking into Sony Pictures Entertainment's computers and the Chinese military of cyber-attacking several U.S. companies. "The infiltration of the Bowman Avenue dam represents a frightening new frontier in cybercrime," U.S. Attorney Preet Bharara of the Southern District of New York said Thursday. "These were no ordinary crimes, but calculated attacks by groups with ties to Iran's Islamic Revolutionary Guard and designed specifically to harm America and its people."
Much U.S. infrastructure is privately owned and poorly defended, given the lack of a major attack and the resulting reluctance to spend money defending against a putative threat. "These sectors may be particularly vulnerable to cyberattack because they rely on open-source software or hardware, third-party utilities, and interconnected networks," the Congressional Research Service warns.
The ability to run such systems remotely, as well as conduct maintenance and update software via the web itself, offers hackers all the access they need. Such networks are particularly tempting because they often control operations, and not merely information, potentially magnifying the impact of any attack on them. "Attacks against operations technology are different than information technology attacks because OT

*(*Continued On The Following Page)*

attacks can produce kinetic effects"—physical destruction—that CRS report noted with studied understatement.
Given the success of Stuxnet, it should come as little surprise that Iran is engaging in cyber warfare. Tehran is believed to be targeting the controls "that operate and monitor our electrical grid," a report by the cyber-security firm Norse Corp. and the American Enterprise Institute warned in a 2015 report. "It seems clear that elements within Iran are working to build a database of vulnerable systems in the U.S., damage to which could cause severe harm to the U.S. economy and citizens."

Chinese National Pleads Guilty to Conspiracy to Hack into U.S. Defense Contractor's Systems to Steal Sensitive Military Information

Department of Justice
Office of Public Affairs
FOR IMMEDIATE RELEASE
Wednesday, March 23, 2016
A Chinese national pleaded guilty today to participating in a years-long conspiracy to hack into the computer networks of major U.S. defense contractors, steal sensitive military and export-controlled data and send the stolen data to China.
Su Bin, also known as Stephen Su and Stephen Subin, 50, a citizen and resident of the People's Republic of China, pleaded guilty before U.S. District Judge Christina A. Snyder of the Central District of California.
The guilty plea was announced by Assistant Attorney General for National Security John P. Carlin, U.S. Attorney Eileen M. Decker of the Central District of California, Assistant Director Jim Trainor of the
FBI's Cyber Division and Assistant Director in Charge David Bowdich of the FBI's Los Angeles Division.

A criminal complaint filed in 2014 and subsequent indictments filed in Los Angeles charged Su, a China-based businessman in the aviation and aerospace fields, for his role in the criminal conspiracy to steal military technical data, including data relating to the C-17 strategic transport aircraft and certain fighter jets produced for the U.S. military. Su was initially arrested in Canada in July 2014 on a warrant issued in relation to this case. Su ultimately waived extradition and consented to be conveyed to the United States in February 2016.
"Su Bin admitted to playing an important role in a conspiracy, originating in China, to illegally access sensitive military data, including data relating to military aircraft that are indispensable in keeping our military personnel safe," said Assistant Attorney General Carlin. "This plea sends a strong message that stealing from the United States and our companies has a significant cost; we can and will find these criminals and bring them to justice. The National Security Division remains sharply focused on disrupting cyber threats to the national security, and we will continue to be relentless in our pursuit of those who seek to undermine our security."

*(*Continued On The Following Column)*

"Protecting our national security is the highest priority of the U.S. Attorney's Office, and cybercrime represents one of the most serious threats to our national security," said U.S. Attorney Decker. "The innovative and tireless work of the prosecutors and investigators in this case is a testament to our collective commitment to protecting our nation's security from all threats. Today's guilty plea and conviction demonstrate that these criminals can be held accountable no matter where they are located in the world and that we are deeply committed to protecting our sensitive data in order to keep our nation safe."

"Cyber security is a top priority not only for the FBI but the entire U.S. government," said Assistant Director Trainor. "Our greatest strength is when we harness our capabilities to work together, and today's guilty plea demonstrates this. Our adversaries' capabilities are constantly evolving, and we will remain vigilant in combating the cyber threat."

"This investigation demonstrates the FBI's resolve in holding foreign cyber actors accountable regardless of where they reside," said Assistant Director in Charge Bowdich. "Cybercrime investigators in Los Angeles are among the finest and their efforts toward preserving America's national security in this case should be commended."

In the plea agreement filed yesterday in the U.S. District Court of the Central District of California, Su admitted to conspiring with two persons in China from October 2008 to March 2014 to gain unauthorized access to protected computer networks in the United States, including computers belonging to the Boeing Company in Orange County, California, to obtain sensitive military information and to export that information illegally from the United States to China.
As part of the conspiracy, Su would e-mail the co-conspirators with guidance regarding what persons, companies and technologies to target during their computer intrusions. One of Su's co-conspirators would then gain access to information residing on computers of U.S. companies and email Su directory file listings and folders showing the data that the co-conspirator had been able to access. Su then directed his co-conspirator as to which files and folders his co-conspirator should steal. Once the co-conspirator stole the data, including by using techniques to avoid detection when hacking the victim computers, Su translated the contents of certain stolen data from English into Chinese. In addition, Su and his co-conspirators each wrote, revised and emailed reports about the information and technology they had
acquired by their hacking activities, including its value, to the final beneficiaries of their hacking activities.

Su's plea agreement makes clear that the information he and his co-conspirators intentionally stole included data listed on the U.S. Munitions List contained in the International Traffic in Arms Regulations. Su also admitted that he engaged in the

(*Continued On The Following Page)

crime for the purpose of financial gain and specifically sought to profit from selling the data the he and his co-conspirators illegally acquired.

Su faces a maximum sentence of five years in prison and a fine of $250,000 or twice the gross gain or gross loss resulting from the offense, whichever is greatest. Judge Snyder is scheduled to sentence Su on July 13, 2016.

The case is being investigated by the FBI Los Angeles Field Office's Cyber Division with assistance from the U.S. Air Force's Office of Special Investigations.

This case is being prosecuted by Assistant U.S. Attorney Anthony J. Lewis of the Central District of California and Trial Attorney Casey Arrowood and Senior Trial Attorney Robert E. Wallace of the National Security Division's Counterintelligence and Export Control Section, with support from Lisa Roberts of the Justice Department's Office of International Affairs.

Computer Hacking Conspiracy Charges Unsealed Against Members of Syrian Electronic Army

Department of Justice
Office of Public Affairs
FOR IMMEDIATE RELEASE
Tuesday, March 22, 2016

Two Fugitives Believed to be in Syria Added to FBI Cyber's Most Wanted

Three Syrian nationals, all current or former members of the Syrian Electronic Army (SEA), were charged with multiple conspiracies related to computer hacking, according to two criminal complaints unsealed today in the U.S. District Court of the Eastern District of Virginia.

The announcement was made by Assistant Attorney General for National Security John P. Carlin, U.S. Attorney Dana J. Boente of the Eastern District of Virginia, Assistant Director James Trainor of the FBI's Cyber Division and Assistant Director in Charge Paul M. Abbate of the FBI's Washington Field Office.

Ahmad Umar Agha, 22, known online as "The Pro," and Firas Dardar, 27, known online as "The Shadow," were charged with a criminal conspiracy relating to: engaging in a hoax regarding a terrorist attack; attempting to cause mutiny of the U.S. armed forces; illicit possession of authentication features; access device fraud; unauthorized access to, and damage of, computers; and unlawful access to stored communications. Dardar and Peter Romar, 36, also known as Pierre Romar, were separately charged with multiple conspiracies relating to: unauthorized access to, and damage of, computers and related extortionate activities; receiving the proceeds of extortion; money laundering; wire fraud; violations of the Syrian Sanctions Regulations;

According to allegations in the first complaint, beginning in or around 2011, Agha and Dardar engaged in a multi-year criminal conspiracy under the name "Syrian Electronic Army" in support of the Syrian Government and President Bashar al-Assad. The conspiracy was dedicated to spear-phishing and compromising the computer systems of the U.S. government, as well as international organizations, media organizations and other private-sector entities that the SEA deemed as having been antagonistic toward the Syrian Government. When the conspiracy's spear-phishing efforts were successful, Agha and Dardar would allegedly use stolen usernames and passwords to deface websites, redirect domains to sites controlled or utilized by the conspiracy, steal email and hijack social media accounts. For example, starting in 2011, the conspirators repeatedly targeted computer systems and employees of the Executive Office of the President (EOP). Despite these efforts, at no time was an EOP account or computer system successfully compromised. Additionally, in April 2013, a member of the conspiracy compromised the Twitter account of a prominent media organization and released a tweet claiming that a bomb had exploded at the White House and injured the President. In a later 2013 intrusion, through a third-party vendor, the conspirators gained control over a recruiting website for the U.S. Marine Corps and posted a defacement encouraging U.S. marines to "refuse [their] orders."

Today, the FBI announced that it is adding Agha and Dardar to its Cyber Most Wanted and offering a reward of $100,000 for information that leads to their arrest. Both individuals are believed to be residing in Syria. Anyone with information is asked to contact their nearest FBI field office or U.S. Embassy or consulate.

According to allegations in the second complaint, beginning in or around 2013, SEA members Dardar and Romar engaged in multiple conspiracies dedicated to an extortion scheme that involved hacking online businesses in the United States and elsewhere for personal profit. Specifically, the complaint alleges that the conspiracy would gain unauthorized access to the victims' computers and then threaten to damage computers, delete data or sell stolen data unless the victims provided extortion payments to Dardar and/or Romar. In at least one instance, Dardar attempted to use his affiliation with the SEA to instill fear into his victim. If a victim could not make extortion payments to the conspiracy's Syrian bank accounts due to the Syrian Sanctions Regulations or other international sanctions regulations, Romar would act as an intermediary in an attempt to evade those sanctions.

"The Syrian Electronic Army publicly claims that its hacking activities are conducted in support of the embattled regime of Syrian President Bashar al-Assad," said Assistant Attorney General Carlin. "While some of the activity sought to harm the economic and national security of the United States in the name of Syria, these detailed allegations reveal that the members also used extortion to try to line their own pockets at the expense of law-abiding people all over the world. The allegations in the complaint demonstrate that the line between ordinary criminal hackers and potential national security threats is increasingly blurry."

*(*Continued On The Following Column)*

*(*Continued On The Following Page)*

“The tireless efforts of U.S. prosecutors and our investigative partners have allowed us to identify individuals who have been responsible for inflicting damage on U.S. government and private entities through computer intrusions,” said U.S. Attorney Boente. “Today’s announcement demonstrates that we will continue to pursue these individuals no matter where they are in the world.”
“Cybercriminals cause significant damage and disruption around the world, often under the veil of anonymity,” said Assistant Director Trainor. “As this case shows, we will continue to work closely with our partners to identify these individuals and bring them to justice, regardless of where they are.”
“These three members of the Syrian Electronic Army targeted and compromised computer systems in order to provide support to the Assad regime as well as for their own personal monetary gain through extortion,” said Assistant Director in Charge Abbate. “As a result of a thorough cyber investigation, FBI agents and analysts identified the perpetrators and now continue to work with our domestic and international partners to ensure these individuals face justice in the United States. I want to thank the dedicated FBI personnel, federal prosecutors, and our law enforcement partners for their tremendous efforts to ensure on-line criminal activity is countered, U.S. cyber infrastructure is safeguarded, and violators are held accountable under the law.”
The case is being investigated by the FBI’s Washington Field Office, with assistance from the NASA Office of the Inspector General, Department of State Bureau of Diplomatic Security and other law enforcement agencies. The case is being prosecuted by Assistant U.S. Attorneys Jay V. Prabhu and Maya D. Song of the Eastern District of Virginia, and Special Assistant U.S. Attorney Brandon Van Grack and Trial Attorneys Scott McCulloch and Nathan Charles

Export Notice

Web Notice: Policy on Exports to Sri Lanka (05.04.16) Licensing restrictions relating to Sri Lanka articulated in §7044(e) of the Consolidated Appropriations Act, 2015, Pub. L. No. 113-235, and in previous appropriations acts, were not carried forward in §7044(e) of the Consolidated Appropriations Act, 2016, Pub. L. No. 114-113. Effective immediately the Directorate of Defense Trade Controls (DDTC) will review applications for licenses to export or temporarily import defense articles and defense services to or from Sri Lanka under the International Traffic in Arms Regulations (ITAR) on a case-by-case basis. DDTC will publish a Federal Register notice to implement a conforming update to ITAR §126.1(n).

Exclusive: North Korea reveals alleged U.S. prisoner to CNN in Pyongyang

Pyongyang, North Korea (CNN) Is North Korea holding an American prisoner? That's what a man CNN spoke to in Pyongyang claims.

As tensions on the Korean peninsula continued to rise and Seoul and Washington officials discussed the potential deployment of more troops to South Korea, officials in Pyongyang gave CNN exclusive access to a man North Korea claims is a U.S. citizen arrested on espionage charges.

Speaking to CNN's Will Ripley, the man identified himself as Kim Dong Chul, a naturalized American, who said he used to live in Fairfax, Virginia.

"I'm asking the U.S. or South Korean government to rescue me," Kim said during an interview at a hotel in the North Korean capital.

Kim, 62, was frogmarched into the room by stony-faced guards, who insisted that the interview be conducted in Korean, through an official translator.
The translation was later independently corroborated by CNN.

Kim told CNN that in 2001 he moved to Yanji, a city near the Chinese-North Korean border that acts as a trade hub between the two countries.

From Yanji, Kim said he commuted daily to Rason, a special economic zone on the North Korean side of the border, where he served as president of a company involved in international trade and hotel services.

According to Kim, he spied on behalf of "South Korean conservative elements," for which he was arrested in October 2015.

"I was tasked with taking photos of military secrets and 'scandalous' scenes," he said.

Kim named a number of South Koreans he said "injected me with a hatred towards North Korea."

"They asked me to help destroy the (North Korean) system and spread propaganda against the government."

According to Kim, North Korean officials said they had been monitoring his activities since 2009, two years after he established his cross-border business.

He started working as a spy in April 2013, bribing local residents to "gather important materials," which he smuggled into China or South Korea.

(*Continued On The Following Page)

Asked whether he worked for the U.S. at any time, Kim said categorically that he did not.

Kim was arrested in October 2015 while he was meeting a source to obtain a USB stick and camera used to gather military secrets.

The source, a 35-year-old former North Korean soldier, was also arrested. Kim said he did not know the other man's fate.

During the almost two years of spying in North Korea, Kim only made around $5,300 (35,000 yuan).

Asked why he would risk his freedom for such a relatively paltry sum of money, Kim said that "it wasn't about the money."

Kim left a wife and two daughters behind in China, with whom he has had no contact since his detention. Repeated attempts to reach his wife using a phone number provided by Kim were unsuccessful.

Kim's claims were made in the presence of North Korean officials and CNN cannot determine whether they were made under duress.

If true, Kim would be the only U.S. citizen held prisoner in North Korea, a fact not revealed until today.

Americans Kenneth Bae and Matthew Miller were released by Pyongyang in November 2014. By that point, Bae had spent more than two years in prison in North Korea.

Hours after the interview with CNN's crew, North Korean authorities provided his passport for inspection.

The U.S. State Department said they could not confirm whether Kim is a U.S. citizen, telling CNN that "speaking publicly about specific purported cases of detained Americans can complicate our tireless efforts to secure their freedom."

On Saturday, CNN spoke to jailed Canadian pastor Hyeon Soo Lim, who said that he hoped "to go home some day."

Kim appeared in good health, and said he was getting proper nourishment and three meals a day.

As is the norm for international prisoners who haven't yet been charged, Kim said he was being held in a Pyongyang hotel, where he has access to local newspapers and television.

He was aware of North Korea's purported hydrogen bomb test, carried out on January 6, saying that it meant it was now time "for the U.S. government to drop its hostile policies against North Korea."

*(*Continued On The Following Column)*

"Seeing that this H-bomb test has succeeded, now is the time to abandon hostile policies and work to help North Korea," he said.

"The U.S. needs to find a way to reconcile with North Korea. I think the main way to do that is with a peace treaty."

Asked about the similarity of his statements to North Korean propaganda and whether any of them had been rehearsed or pre-scripted, Kim said that they had not, and accused Western media of "misunderstanding" the situation in the country.

Westerners held previously in North Korea have said their confessions were given under pressure from the state.

Tensions on the Korean peninsula are at their highest for some time, with South Korea resuming propaganda broadcasts across the demilitarized zone. Pyongyang regards such broadcasts as tantamount to an act of war and has fired on the giant speakers used for them in the past.

On Sunday, a U.S. B-52 bomber flew over Osan, South Korea in what officials said was a show of solidarity with Seoul following the purported nuclear test. The U.S. bomber was flanked by a South Korean F-15.

Weighing The Good And The Bad Of Autonomous Killer Robots In Battle

In his lab at George Mason University in Virginia, Sean Luke has all kinds of robots: big ones with wheels; medium ones that look like humans. And then he has a couple of dozen that look like small, metal boxes.

He and his team at the Autonomous Robotics Lab are training those little ones to work together without the help of a human.

In the future, Luke and his team hope those little robots can work like ants — in teams of hundreds, for example, to build houses, or help search for survivors after a disaster.

"These things are changing very rapidly and they're changing much faster than we sort of expected them to be changing recently," Luke says.

New algorithms and huge new databases are allowing robots to navigate complex spaces, and artificial intelligence just achieved a victory few thought would ever happen: A computer made by Google beat a professional human in a match of Go

(*Continued On The Following Page)

It doesn't take much imagination to conjure a future in which a swarm of those robots are used on a battlefield. And if that sounds like science fiction, it's not.

Earlier this month representatives from more than 82 countries gathered in Geneva to consider the repercussions of that kind of development. In the end, they emerged with a recommendation: The key U.N. body that sets norms for weapons of war should put killer robots on its agenda.

A 'Moral Threshold'

Human Rights Watch and Harvard Law School's International Human Rights Clinic added to the urgency of the meeting by issuing a report calling for a complete ban on autonomous killer robots.

Bonnie Docherty, who teaches at Harvard Law School and was the lead author of the report, says the technology must be stopped before humanity crosses what she calls a "moral threshold."

"[Lethal autonomous robots] have been called the third revolution of warfare after gunpowder and nuclear weapons," she says. "They would completely alter the way wars are fought in ways we probably can't even imagine."

Docherty says killer robots could start an arms race and also obscure who is held responsible for war crimes. But above all, she says, there is the issue of basic human rights.

"It would undermine human dignity to be killed by a machine that can't understand the value of human life," she says.

Paul Scharre, who runs a program on ethical autonomy at the Center for a New American Security and was also in Geneva for the talks, says that it's pretty clear that nobody wants "Cylons and Terminators."

In truth, he says, the issue of killer robots is more complicated in reality than it is in science fiction.

Take, for example, the long-range anti-ship missile Lockheed Martin is developing for the U.S. military. The LRASM can lose contact with its human minders yet still scour the sea with its sensors, pick a target and slam into it.

"It sounds simple to say things like: 'Machines should not make life-or-death decisions.' But what does it mean to make a decision?" Scharre asks. "Is my Roomba making a decision when it bounces off the couch and wanders around? Is a land mine making a decision? Does a torpedo make a decision?"

'Meaningful Human Control'

*(*Continued On The Following Column)*

Scharre helped write U.S. policy on killer robots and he likes where things ended up.

Department of Defense Directive 3000.09 requires a high-ranking Defense official to approve unusual uses of autonomous technology and also calls for those systems to always keep "appropriate levels of human judgment over the use of force."

Proponents of a ban say that policy leaves too much wiggle room. They advocate that all military weapons maintain "meaningful human control."
Georgia Tech's Ron Arkin, who is one of the country's leading roboethicists, says hashing out that distinction is important but the potential benefits of killer robots should not be overlooked.

"They can assume far more risk on behalf of a noncombatant than any human being in their right mind would," he says. "They can potentially have better sensors to cut through the fog of war. They can be designed without emotion — such as anger, fear, frustration — which causes human beings, unfortunately, to err."

Arkin says robots could become a new kind of precision-guided weapon. They could be sent into an urban environment, for example, to take out snipers. He says that's probably far into the future, but what he knows right now is that too many innocent people are still being killed in war.

"We need to do something about that," he says. "And technology affords one way to do that and we should not let science fiction cloud our judgment in terms of moving forward."

Arkin says one day killer robots could be so precise that it might become inhumane not to use them.

The next meeting in Geneva is set for December, when a U.N. group will decide whether to formally start developing new international law governing killer robots. Since the last meeting, 14 countries have joined in calling for a total ban.

CHINA AND RUSSIA URGE U.S. TO ABANDON KOREA MISSILE DEFENSE PLANS

CHINA AND RUSSIA URGED THE UNITED STATES ON FRIDAY NOT TO INSTALL A NEW ANTI-MISSILE SYSTEM IN SOUTH KOREA, AFTER WASHINGTON SAID IT WAS IN TALKS WITH SEOUL IN THE WAKE OF NUCLEAR ARMS AND MISSILE TESTS BY NORTH KOREA.

*(*Continued On The Following Page)*

The United States and South Korea have begun talks on possible deployment of the Terminal High Altitude Area Defense (THAAD) system after North Korea tested its fourth nuclear bomb on January 6 and conducted missile tests.

The nuclear test and missile launches are in violation of U.N. resolutions against North Korea backed by Russia and China. U.S. and South Korean officials have expressed concern that the North could attempt a fifth nuclear test in a show of strength ahead of its Workers' Party congress, which begins on May 6.

Speaking at joint press briefing with Russian Foreign Minister Sergei Lavrov, Chinese Foreign Minister Wang Yi said the United States should respect "legitimate concerns" of China and Russia over the missile system.North Korea test-fired what appeared to be two intermediate range ballistic missiles on Thursday, but both failed, the U.S. military said.

"This move goes beyond the defensive needs of the relevant countries. If it is deployed it will directly impact China's and Russia's respective strategic security," Wang said.

"Not only does it threaten the resolution of the peninsula nuclear issue, it quite possibly could pour oil on the fire of an already tense situation, and even destroy strategic equilibrium on the peninsula."

North Korea's actions should not be used as an excuse to make moves that would escalate tensions, especially the U.S. deployment of an anti-missile system, Lavrov said, according to an interpretation in Chinese.

North Korea's drive to develop a nuclear weapons capability has angered China, Pyongyang's sole major diplomatic and economic supporter. But Beijing fears THAAD and its radar have a range that would extend far beyond the Korean peninsula and into China.

Chinese President Xi Jinping said on Thursday that Beijing would not allow war and chaos to break out on the Korean peninsula.

North and South Korea remain technically at war after their 1950-53 conflict ended in a truce, rather than a treaty. The North routinely threatens to destroy South Korea and its major ally, the United States.

SEATTLE: Boeing visionary Nicole Piasecki looks to next century

BUSINESS JOURNAL PHOTO | Anthony BolanteSEATTLE — Nicole Piasecki grew up running around her father's helicopter factory with her two brothers.

*(*Continued On The Following Column)*

Her father, Frank Piasecki, developed the twin-rotor technology that powers Chinook helicopters Boeing now makes for the military. He started taking his daughter to his Philadelphia helicopter factory when she was just six years old. Frank Piasecki must have been an inspiring presence – all three of his children ended up with careers in the aerospace industry.

While her brothers have gone on to run their late father's company, Piasecki Aircraft Corp., Nicole Piasecki has spent 25 years rising through the ranks at Boeing. She started as an engineer on the 777 line and within two years, moved into management. She has since emerged as one of the aerospace industry's most forward-thinking leaders.

Piasecki is now vice president and general manager of propulsion for Boeing Commercial Airplanes, acting as the liaison between Boeing and the jet engine makers that supply it.

"We want to create the next 100 years," she said. "That's what we're focused on."

But maintaining leadership amid a growing list of competitors will require new technologies and strategies. That's something Piasecki is confident Boeing can develop.

"We have to ... create a culture that enables risk taking, that embraces differences of thought," she said. "In those tensions you create innovation and better solutions."

That means building a culture at Boeing where employees feel they can take risks and even fail without being punished for ideas that don't work.

"Because if you don't allow failure," she said, "nobody wants to have a new idea and try it."Boeing leadership also needs to be more aware of the competitive landscape and the growing threats – including smaller companies such as Bombardier, and overseas manufacturers – to the company's dominance, she said.

"I lived through the 1990s when we were a little bit in denial about Airbus," she said. "We finally woke up at the end of the '90s and realized 'We have a real competitor here.'"

To anticipate threats, Piasecki said, Boeing has to cultivate a long view.

"We have to earn our way every day, and keep our sights not only on what we have to deliver today," she said. "I believe we have to be looking 30, 50 years out about where the world is going, and solving problems in the context of 30 to 50 years, not just this year and next year."

*(*Continued On The Following Page)*

China, for example, is developing its own jetliner industry, which could eventually become a real threat to Boeing if and when China begins building wide-body jets. This is especially true, as Chinese airlines are some of Boeing's biggest customers.

"It's not just about putting an airplane technically into the market," Piasecki said. "I'm confident the Chinese will deliver an airplane that flies into the marketplace. But I am more confident that Boeing will work to stay ahead of our competition in terms of technology, talent, business processes ... to go in a direction our competition can't see."

Connect with Nicole Piasecki: LinkedIn

Commercial Aircraft MRO Market $65,490m in 2016

The commercial aircraft maintenance, repair & overhaul (MRO) market is an essential element of commercial air transport ensuring that aircraft are maintained in conditions of airworthiness that are determined by international and national regulators. The market is influenced by trends of the wider air transport sector with growth and aircraft fleet expansion generating opportunities for MRO services to accommodate an increase in capacity.

The commercial aircraft MRO market is calculated to be worth $65,490m in 2016. Overall, the market is mature and continues to be influenced by a number of factors related to the wider air transport industry. Although the global fleet of commercial aircraft is forecast to grow over the next decade, the MRO market is not expected to expand proportionally.

The global fleet will encompass a higher number of next generation aircraft or newer variants of existing types. These aircraft are more reliable and thus require less maintenance in the short term outlook. In some regions, the influx of new aircraft is part of fleet renewal strategies and is replacing older aircraft, resulting in a small net increase. Long term, demand is anticipated to increase as airframes accumulate flight cycles which warrant inspection of airframes and replacement of components in accordance with regulations.

Traditional market players include in-house maintenance divisions of airlines and independent MRO companies. More recently, original equipment manufacturers (OEMs) have increased their presense in the market. On the other hand, there are fewer airlines performing MRO in-house. Overall, this is expected to increase competition in the market, putting pressure on more established players.

28113
Federal Register
Vol. 81, No. 89 / Monday, May 9, 2016 / Notices

DEPARTMENT OF STATE
[Public Notice: 9551]
In the Matter of the Designation of Musa Abu Dawud, aka Moussa Abu Daoud, aka Moussa Bourahla, aka Abou Daoud, aka Bourahla Moussa, as a Specially Designated Global Terrorist Pursuant to Section 1(b) of Executive Order 13224, as Amended Acting under the authority of and in accordance with section 1(b) of Executive Order 13224 of September 23, 2001, as amended by Executive Order 13268 of July 2, 2002, and Executive Order 13284 of January 23, 2003, I hereby determine that the individual known as Moussa Abu Dawud, also known as Moussa Abu Daoud, also known as Moussa Bourahla, also known as Abou Daoud, also known as Bourahla Moussa committed, or poses a significant risk of committing, acts of terrorism that threaten the security of U.S. nationals or the national security, foreign policy, or economy of the United States. Consistent with the determination in section 10 of Executive Order 13224 that ''prior notice to persons determined to be subject to the Order who might have a constitutional presence in the United States would render ineffectual the blocking and other measures authorized in the Order because of the ability to transfer funds instantaneously,'' I determine that no prior notice needs to be provided to any person subject to this determination who might have a constitutional presence in the United States, because to do so would render ineffectual the measures authorized in the Order. This notice shall be published in the Federal Register.
John F. Kerry,
Secretary of State.

DEPARTMENT OF STATE
[Public Notice: 9550]
Bureau of Political-Military Affairs; Modification of Statutory Debarment Imposed Pursuant to Section 127.7(c) of the International Traffic in Arms Regulations—Rocky Mountain Instrument Company
ACTION

Notice.
SUMMARY:
Notice is hereby given that the Department of State will consider license applications for the indirect participation of

*(*Continued On The Following Page)*

Rocky Mountain Instrument Company (''RMI'') in certain transactions subject to the Arms Export Control Act (AECA) (22 U.S.C 2778) without the submission of a transaction exception request as an element of the application.

DATES:

This notice is effective on May 9, 2016.

FOR FURTHER INFORMATION CONTACT:

Sue Gainor, Director, Office of Defense Trade Controls Compliance, Bureau of Political-Military Affairs, U.S. Department of State (202) 632–2785.

SUPPLEMENTARY INFORMATION:

On September 8, 2010, the Department notified the public of a statutory debarment imposed on RMI pursuant to ITAR § 127.7(c) related to RMI's criminal conviction, 75 FR 54692. The notice provided that RMI is ''prohibited from participating directly or indirectly in the export of defense articles, including technical data, or in the furnishing of defense services for which a license or other approval is required.''

Further, the notice provided that:

Exceptions, also known as transaction exceptions, may be made to this debarment determination on a case-by-case basis at the discretion of the Assistant Secretary of State for Political-Military Affairs, after consulting with the appropriate U.S. agencies. However, such an exception would be granted only after a full review of all circumstances, paying particular attention to the following factors: Whether an exception is warranted by overriding U.S. foreign policy or national security interests; whether an exception would further law enforcement concerns that are consistent with the foreign policy or national security interests of the United States; or whether other compelling circumstances exist that are consistent with the foreign policy or national security interests of the United States, and that do not conflict with law enforcement concerns. Even if exceptions are granted, the debarment continues until subsequent reinstatement. Notwithstanding the prohibition on indirect participation referenced in the original notice of statutory debarment, and in conformance with the stated policy and procedures regarding transaction exceptions, based on overriding national security and foreign policy concerns and after a thorough review of the circumstances surrounding the conviction and a finding that appropriate steps have been taken to mitigate law enforcement concerns, the Under Secretary for Arms Control and International Security has determined to approve specific exceptions from the debarment of RMI, available to persons other than RMI but excluding persons acting for or on behalf of RMI in contravention of ITAR § 127.1(d), for the following categories of authorization requests:

1. Applications submitted by persons other than RMI for the export temporary import of defense articles manufactured by RMI (i.e., where RMI is identified as a Source or Manufacturer);

*(*Continued On The Following Column)*

2. Application submitted by persons other than RMI for the export or temporary import of defense articles manufactured by persons other than RMI which incorporate a defense article manufactured by RMI as a component, accessory, attachment, part, firmware, software, or system;
3. The use of other approvals (see ITAR § 120.20) by persons other than RMI for the export or temporary import of defense articles described in categories one (1) and two (2) above; and
4. Applications submitted by persons other than RMI for agreements identified in ITAR Part 124 in which RMI is identified as a U.S. signatory to the agreement.

All requests for authorizations, or use of exemptions, involving RMI that fall within the scope of the specific categories above will be reviewed and action taken by the Directorate of Defense Trade Controls in the ordinary course of business and do not require the submission of a separate transaction exception request, but should include reference to, or a copy of, this notice. Including an explanation of how the proposed transaction falls within the scope of an exception category above will facilitate review of the request.

All requests for authorizations involving RMI that do not fall within the scope of the specific categories above must be preceded by the approval of a transaction exception request by the Department. The decision to grant a transaction exception will be made on a case-by-case basis after a full review of all circumstances. This notice does not provide notice of reinstatement of export privileges for RMI pursuant to the statutory requirements of AECA Sec. 38(g)(4) (22 U.S.C. 2778), nor does this notice provide notice of rescission of the imposition of statutory debarment of RMI pursuant to ITAR § 127.7(c). As required by the statute, the Department will not consider applications from RMI unless accompanied by a specific transaction exception request. Any determination by the Department regarding reinstatement of export privileges for RMI or rescission of the imposition of statutory debarment of RMI will be made in accordance with statutory and regulatory requirements and will be the subject of a separate notice.

Dated: April 25, 2016.
Rose E. Gottemoeller,
Under Secretary, Arms Control and International Security, Department of State.
[FR Doc. 2016–10843 Filed 5–6–16; 8:45 am]
BILLING CODE 4710–25–P

NOTE: In accordance with Title 17 U.S.C. Section 107, this material is distributed without profit or payment for non-profit news reporting and educational purposes only.