EIB World Trade Headlines

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

June 2013 - Volume 5, Issue 9

D-Trade 2 To Undergo Maintenance During July 3, 2013 - July 8, 2013 in Support of Department of State Migration to USXports

(http://www.pmddtc.state.gov/)
June 19, 2013

Industry User Announcement

On July 8, 2013, the Export Control Reform Initiative (http://export.gov/ecr/index.asp) will be advanced as the Department of State, which processes the largest volume of licenses, migrates portions of its license adjudication operations to the Department of Defense's USXports System.

Registered Industry Users will see very little change and will continue to submit license applications through D-Trade 2, as they do today. This migration requires that D-Trade 2 be shut down for maintenance for several days. To reduce the business impact to industry, the cutover will occur during the July 4th holiday weekend. D-Trade 2 will be shut down at Noon on July 3, 2013 and will be unavailable for license application submission until the morning of Monday, July 8 2013.

(Continued below)

NEWSLETTER NOTES

If you try to submit a license application during the maintenance period, you will receive an error message. Please be aware of the following changes after migration to USXports License Application Submission. To see changes click link: http://www.pmddtc.state.gov/

Continue to submit license applications as you have been. There is no change to the submission process.

Tracking Case Status

Case Statuses will continue to be available via D-Trade 2 and MARY. However, the details of statuses contained in these systems have changed. A summary of the changes can be found at this link http://www.pmddtc.state.gov/

Detailed case status is available via DoD's ELISA System

License Decisions

Signed Licenses and decisions will continue to be available via D-Trade 2. The contents of the licenses will not change, but the format of the license will be different. A sample is available at this link http://www.pmddtc.state.gov/

Once the maintenance is completed, a notice will be posted on this web site informing you that the system is available for license application submission. If you have any questions about this activity, please contact the DDTC Help Desk at 202-663-2838 or dtradehelpdesk@state.gov.

Air France-KLM Signs MOU with Rolls-Royce for Trent XWB Engines to Power up to 50 Airbus A350s

In a landmark deal announced at the Paris Air Show today (Wednesday 19 June) Air France-KLM Group has signed a Memorandum of Understanding with Rolls-Royce for Trent XWB engines to power 25 Airbus A350s. The agreement is worth $1.1bn at current list prices.
Air France-KLM also has options covering 25 more A350 XWB aircraft.

Alexandre de Juniac, Chairman and Chief Executive Officer of Air France said: "We're very pleased to have reached agreement with Rolls-Royce for Trent XWB engines to power our fleet of Airbus A350 XWBs. Peter Hartman, President and Chief Executive Officer of KLM, added: "This includes an agreement for the Air France-KLM maintenance organization to work with Rolls-Royce on Trent XWB engine maintenance support."

Eric Schulz, President – Civil Large Engines, Rolls-Royce, said: "We look forward to forging a strong relationship with Air France-KLM group and we're delighted that for the first time their fleet will soon include aircraft powered by a member of our Trent family of engines. This is a great opportunity for us to demonstrate to Air France-KLM the exceptional product efficiency and superior service support benefits that Rolls-Royce Trent customers enjoy."

Source: **Rolls-Royce Plc (LSE: RR.L)**

Government Sets $325 Billion Exports Target for 2013-2014

PTI May 8, 2013, 02.21PM IST

NEW DELHI: The government has set an export target of $325 billion for the current financial year on the back of slowdown in the global markets, Parliament was informed today.

"Government has set an export target of $ 325 billion for the year 2013-14," Minister of State for Commerce and Industry D Purandeswari said in a written reply to the Rajya Sabha.

Researchers Upbeat About U.S. Plan to Ease Export Rules on Space Technology

***by Laura Dattaro* - June 6, 2013, 12:00 PM**

U.S. scientists and companies could soon find it easier to collaborate with international partners on projects involving potentially sensitive spacecraft technologies. The Obama administration has opened public comment on new rules designed to ease government controls on exporting space-related technologies, such as satellites, that could have military applications.

Existing U.S. export controls have drawn criticism from scientists and space industry executives, who say that they have hampered collaboration with foreign colleagues and customers. U.S. export controls have been "a real complication for cooperative space activities," says Jorge Vago, project scientist for the European Space Agency's (ESA's) ExoMars program. And if the new U.S. rules "reclassify spacecraft in such a way that all the singing and dancing that is required at present could be avoided, this would constitute a great step."

The new rules are designed to streamline the process of getting export permits. Now, the U.S. government closely regulates export of space-related technologies under rules known as the International Traffic in Arms Regulations (ITAR), which are overseen by the U.S. Department of State.

(Continued above)

In 1999, responding to a controversy over the alleged theft of U.S. space technologies by China and other nations, Congress passed legislation that required all space-related technologies to be listed and tightly regulated as "munitions" under the ITAR framework, making the United States the only space power with such a policy. Lawmakers also barred the White House from exempting any technologies from the regulations.

Live Chat: The Science of Superman

Thursday 3 p.m. EDT

In practice, the moves meant U.S. companies and researchers seeking a government permit to share technologies with foreign partners faced "a presumption of denial," says Scott Pace, director of the Space Policy Institute at George Washington University (GWU) in Washington, D.C. "If you want to export something the answer is no unless you have a specific waiver or exemption."

Over the years, that stance drew extensive criticism, and in 2010 Congress required the secretaries of defense and state to evaluate the potential dangers and benefits of removing certain space-related items from the munitions list. The resulting report concluded that U.S. export policies were far stiffer than those adopted by other space powers and that they placed "the U.S. satellite industry at a distinct, competitive disadvantage that undermines the U.S. space industrial base to the detriment of U.S. national security." The report also recommended that Congress once again give the president the power to decide which space technologies were listed as munitions.

Last year, Congress did just that, empowering the White House to remove space technologies from the ITAR framework and regulate them instead under the less onerous Export Administration Regulations (EAR) run by the U.S. Department of Commerce. And last month, the Obama administration followed up, identifying a number of space technologies that it wants to reclassify and take off the munitions list as part of a "common sense approach to overhauling the nation's export control system."

(Continued below)

The proposal doesn't list specific products or devices; instead, it focuses on defining capabilities that might make a satellite or space technology valuable to military forces, and not just civilians. That threshold-setting approach means many research-related technologies, such as weather satellites and NASA research probes, will fall off the munitions list, says Mark Mulholland, a senior adviser at the National Oceanic and Atmospheric Administration in Washington, D.C.

In essence, GWU's Pace says, the proposal "takes the entire category [of spacecraft] and, instead of saying all space items are by definition munitions items, it goes back and makes a little more nuanced treatment." The change, he adds, should make the process of getting an export permit from the Commerce Department "easier to deal with." ESA's Vago predicts that "relaxing ITAR for space activities … would be good for both U.S. and European industry."

Public comment on the administration's proposal is due by 8 July.

Distribution of 3-D Plastic Gun Design Banned by U.S. Government

(Thousands of Disobedient Pirate Bay Users Ignore Order)

By STEVEN NELSON
May 10, 2013 RSS Feed Print

After more than 100,000 downloads in two days from the website DEFCAD.org, the Obama administration is struggling to shut down distribution of "3-D" designs for a plastic gun called "The Liberator."

The plastic gun, designed by the Texas-based company Defense Distributed, looks somewhat similar to a grocery store bar code scanner and is theoretically capable of firing a bullet with deadly force. It requires 15 plastic parts printed on an industrial machine and one common metal nail. The U.S. State Department's Office of Defense Trade Controls Compliance warned in a Wednesday letter published by Forbes that the design "should be removed from public access immediately" until the government determines if the product falls under the International Traffic in Arms Regulations - typically invoked to guard against U.S. companies sharing defense and space-related technology with foreigners.

(Continued above)

"Defense Distributed may have released ITAR-controlled technical data without the required prior authorization from the Directorate of Defense Trade Controls (DDTC), a violation of the ITAR," said the letter.

Defense Distributed said in a Thursday tweet, "#DEFCAD has gone dark at the request of the Department of Defense Trade Controls. Take it up with the Secretary of State."
It's virtually impossible, however, to contain the spread of information on the Internet. The Pirate Bay, a famous file-sharing service founded in Sweden, is now the hub of distribution, the website TorrentFreak reports.

As of Friday morning instructions for the gun are being shared by at least 2,001 "seeders" via Pirate Bay. The Pirate Bay "has for close to 10 years been operating without taking down one single torrent due to pressure from the outside. And it will never start doing that," a source within the organization told TorrentFreak.

Forbes reports that the file downloaded via DEFCAD.org was hosted by Mega, a service developed by Internet freedom activist Kim DotCom, whose MegaUpload file-sharing empire was shut down by the FBI in 2012. A defiant DotCom has been successfully fighting the legal case against him - and won an apology from New Zealand's prime minister - after a dramatic raid on his home by U.S. and New Zealand law enforcement last year.

Making one of the plastic guns requires an $8,000 Stratasys Dimension SST 3D printer, The Guardian reports.

(Continued below)

The social media website Reddit has been a springboard for information about the gun, with the site's users upvoting en masse new developments. Gun control proponent Sen. Chuck Schumer, D-N.Y., called the gun "stomach-churning" and proposed regulations to ban them on May 5, before the instructions were widely distributed online.

British 3-D printer Jonathan Rowley said in a Wednesday blog post that the gun could prove costly in more ways than one to users. Rowley reportedly refused requests from The Mail on Sunday and The Telegraph to print the gun, fearing that the weapon might actually kill users.

How Hackers Can Turn the Internet of Things into a Weapon

GNC
May 3, 2013

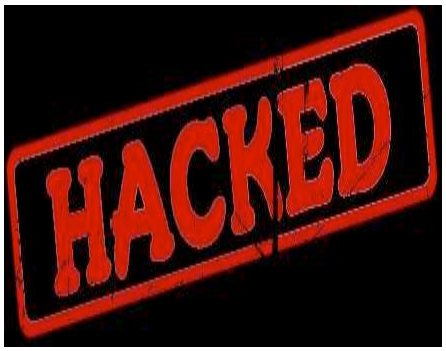
We are living in world of increasingly smart devices. Not really intelligent; just smart enough to be dangerous. As more devices become IP-enabled, they contribute to the pool of things that can be recruited into botnets or other platforms used for distributed attacks. Distributing attacks make it more difficult to trace the source of the attack and also makes it easier to overwhelm a target. In the past year, distributed denial of service has become the attack of choice for activists and blackmailers.

Prolexic, a DDOS security company, has published a white paper on Distributed Reflection Denial of Service (DrDOS) attacks that focuses on a handful of protocols, including the Simple Network Management Protocol. SNMP is an application layer (Layer 7) protocol commonly used to manage devices with IP addresses.

(Continued above)

"Unlike other DDOS and DrDOS attacks, SNMP attacks allow malicious actors to hijack unsecured network devices — such as routers, printers, cameras, sensors and other devices —and use them as bots to attack third parties," the report points out.

To review the rest of the article please click on the link: http://gcn.com/blogs/cybereye/2013/05/how-hackers-turn-internet-of-things-into-weapon.aspx?s=gcntech_060513



"I venture to suggest that patriotism is not a short and frenzied outburst of emotion but the tranquil and steady dedication of a lifetime."

Adali Stevenson

Why Wiping Decommissioned IT Assets Should be a Must

HEISE SECURITY
May 7, 2013

We all know the enormous amount of data a modern computer can store on the cheap, so the proper destruction of that data is essential before the workstation leaves the organization. Unfortunately, many tend to disregard this issue and simply swap the computers with new ones or merely format the drives without securely wiping the data.

A few years ago, British researchers found top-secret U.S. missile defense system data while examining 300 hard drives bought at computer auctions, computer fairs and eBay. I'm sure that if someone did a similar research today, they would still discover sensitive data leaking into the wild.

About 99% of problems happen before a disposal vendor touches equipment. No vendor can destroy data if they don't receive an asset, which is why we strongly encourage clients to destroy data before any move. Better safe than sorry. Of course, disposal vendors should destroy data (again) regardless," says Kyle Marks, CEO of Retire-IT.

Retire-IT looked at tracking data from 1072 corporate disposal projects encompassing 233 clients to destroy data before any move. Better safe than sorry. Of course, disposal vendors should destroy data (again) regardless," says Kyle Marks, CEO of Retire-IT. Retire-IT looked at tracking data from 1072 corporate disposal projects encompassing 233 different companies.

Here are two shocking figures:

* 4 out of 5 projects (81.5%) had at least one missing asset. Contrast that with only 1 out of 8 (11.6%) had a negative variance. The devil is in the details, but nobody looks very closely.

* Only 79% of the serial numbers could be matched. This is when they allowed subjective matching. Without subjective matching, only 58% of serial numbers could be matched.

(Continued above)

After the identification of data-sensitive equipment that requires appropriate handling before disposal, there are different software and hardware solutions to automate the process of wiping the data, preventing that confidential information fall into the wrong hands.

To review the rest of the article please click on the link: http://www.net-security.org/secworld.php?id=14875

Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyber-Spies

THE WASHINGTON POST
May 27, 2013

Designs for many of the nation's most sensitive advanced weapons systems have been compromised by Chinese hackers, according to a report prepared for the Pentagon and to officials from government and the defense industry.

Among more than two dozen major weapons systems whose designs were breached were programs critical to U.S. missile defenses and combat aircraft and ships, according to a previously undisclosed section of a confidential report prepared for Pentagon leaders by the Defense Science Board. The systems named in a report by the Defense Science Board includes some critical to U.S. missile defense.

Experts warn that the electronic intrusions gave China access to advanced technology that could accelerate the development of its weapons systems and weaken the U.S. military advantage in a future conflict. The Defense Science Board, a senior advisory group made up of government and civilian experts, did not accuse the Chinese of stealing the designs. But senior military and industry officials with knowledge of the breaches said the vast majority were part of a widening Chinese campaign of espionage against U.S. defense contractors and government agencies.

(Continued below)

The significance and extent of the targets help explain why the Obama administration has escalated its warnings to the Chinese government to stop what Washington sees as rampant cyber theft.

In January, the advisory panel warned in the public version of its report that the Pentagon is unprepared to counter a full-scale cyber-conflict. The list of compromised weapons designs is contained in a confidential version, and it was provided to The Washington Post.

Some of the weapons form the backbone of the Pentagon's regional missile defense for Asia, Europe and the Persian Gulf. The designs included those for the advanced Patriot missile system, known as PAC-3; an Army system for shooting down ballistic missiles, known as the Terminal High Altitude Area Defense, or THAAD; and the Navy's Aegis ballistic-missile defense system.

Also identified in the report are vital combat aircraft and ships, including the F/A-18 fighter jet, the V-22 Osprey, the Black Hawk helicopter and the Navy's new Littoral Combat Ship, which is designed to patrol waters close to shore.

Also on the list is the most expensive weapons system ever built — the F-35 Joint Strike Fighter, which is on track to cost about $1.4 trillion. The 2007 hack of that project was reported previously.

China, which is pursuing a comprehensive long-term strategy to modernize its military, is investing in ways to overcome the U.S. military advantage — and cyber-espionage is seen as a key tool in that effort, the Pentagon noted this month in a report to Congress on China. For the first time, the Pentagon specifically named the Chinese government and military as the culprit behind intrusions into government and other computer systems.

As the threat from Chinese cyber-espionage has grown, the administration has become more public with its concerns. In a speech in March, Thomas Donilon, the national security adviser to President Obama, urged China to control its cyber-activity. In its public criticism, the administration has avoided identifying the specific targets of hacking.

(Continued above)

But U.S. officials said several examples were raised privately with senior Chinese government representatives in a four-hour meeting a year ago. The officials, who spoke on the condition of anonymity to describe a closed meeting, said senior U.S. defense and diplomatic officials presented the Chinese with case studies detailing the evidence of major intrusions into U.S. companies, including defense contractors.

In addition, a recent classified National Intelligence Estimate on economic cyber-espionage concluded that China was by far the most active country in stealing intellectual property from U.S. companies.

The Chinese government insists that it does not conduct -cyber- espionage on U.S. agencies or companies, and government spokesmen often complain that Beijing is a victim of U.S. cyber attacks.

Obama is expected to raise the issue when he meets with Chinese President Xi Jinping next month in California.

A spokesman for the Pentagon declined to discuss the list from the science board's report. But the spokesman, who was not authorized to speak on the record, said in an e-mail, "The Department of Defense has growing concerns about the global threat to economic and national security from persistent cyber-intrusions aimed at the theft of intellectual property, trade secrets and commercial data, which threatens the competitive edge of U.S. businesses like those in the Defense Industrial Base."

The confidential list of compromised weapons system designs and technologies represents the clearest look at what the Chinese are suspected of targeting. When the list was read to independent defense experts, they said they were shocked by the extent of the cyber-espionage and the potential for compromising U.S. defenses.

"That's staggering," said Mark Stokes, executive director of the Project 2049 Institute, a think tank that focuses on Asia security issues. "These are all very critical weapons systems, critical to our national security. When I hear this in totality, it's breathtaking."

(Continued below)

The experts said the cyber theft creates three major problems. First, access to advanced U.S. designs gives China an immediate operational edge that could be exploited in a conflict. Second, it accelerates China's acquisition of advanced military technology and saves billions in development costs. And third, the U.S. designs can be used to benefit China's own defense industry. There are long-standing suspicions that China's theft of designs for the F-35 fighter allowed Beijing to develop its version much faster.

"You've seen significant improvements in Chinese military capabilities through their willingness to spend, their acquisitions of advanced Russian weapons, and from their cyber-espionage campaign," said James A. Lewis, a cyber-policy expert at the Center for Strategic and International Studies. "Ten years ago, I used to call the PLA [People's Liberation Army] the world's largest open-air military museum. I can't say that now."

The public version of the science board report noted that such cyber-espionage and cyber-sabotage could impose "severe consequences for U.S. forces engaged in combat." Those consequences could include severed communication links critical to the operation of U.S. forces. Data corruption could misdirect U.S. operations. Weapons could fail to operate as intended. Planes, satellites or drones could crash, the report said.

In other words, Stokes said, "if they have a better sense of a THAAD design or PAC-3 design, then that increases the potential of their ballistic missiles being able to penetrate our or our allies' missile defenses."

Winslow T. Wheeler, director of the Straus Military Reform Project at the Project on Government Oversight, made a similar point. "If they got into the combat systems, it enables them to understand it to be able to jam it or otherwise disable it," he said. "If they've got into the basic algorithms for the missile and how they behave, somebody better get out a clean piece of paper and start to design all over again."

The list did not describe the extent or timing of the penetrations. Nor did it say whether the theft occurred through the computer networks of the U.S. government, defense contractors or subcontractors.

(Continued above)

Privately, U.S. officials say that senior Pentagon officials are frustrated by the scale of cyber theft from defense contractors, who routinely handle sensitive classified data. The officials said concerns have been expressed by Gen. Martin Dempsey, chairman of the Joint Chiefs of Staff, and Adm. James A. Winnefeld Jr., the vice chairman, as well as Gen. Keith Alexander, director of the National Security Agency.

"In many cases, they don't know they've been hacked until the FBI comes knocking on their door," said a senior military official who was not authorized to speak on the record. "This is billions of dollars of combat advantage for China. They've just saved themselves 25 years of research and development. Its nuts." In an attempt to combat the problem, the Pentagon launched a pilot program two years ago to help the defense industry shore up its computer defenses, allowing the companies to use classified threat data from the National Security Agency to screen their networks for malware. The Chinese began to focus on subcontractors, and now the government is in the process of expanding the sharing of threat data to more defense contractors and other industries.

An effort to change defense-contracting rules to require companies to secure their networks or risk losing Pentagon business stalled last year. But the 2013 Defense Authorization Act has a provision that requires defense contractors holding classified clearances to report intrusions into their networks and allow access to government investigators to analyze the breach.

The systems on the science board's list are built by a variety of top defense contractors, including Boeing, Lockheed Martin, Raytheon and Northrop Grumman. None of the companies would comment about whether their systems have been breached.

But Northrop Grumman spokes-man Randy Belote acknowledged the company "is experiencing greater numbers of attempts to penetrate its computer networks" and said the firm is "vigilant" about protecting its networks.

(Continued below)

A Lockheed Martin official said the firm is "spending more time helping deal with attacks on the supply chain" of partners, subcontractors and suppliers than dealing with attacks directly against the company. "For now, our defenses are strong enough to counter the threat, and many attackers know that, so they go after suppliers. But of course they are always trying to develop new ways to attack."

The Defense Science Board report also listed broad technologies that have been compromised, such as drone video systems, nanotechnology, tactical data links and electronic warfare systems — all areas where the Pentagon and Chinese military are investing heavily. "Put all that together — the design compromises and the technology theft — and it's pretty significant," Stokes said.

China's Supreme People's Court to Hear AMSC's Cases against Sinovel on May 29, 2013

GLOBE NEWSWIRE
May 24, 2013

Devens, Mass - AMSC, a global solutions provider serving the wind and power grid industry, today announced that China's Supreme People's Court has scheduled a hearing for May 29, 2013 to review the jurisdiction of AMSC's software copyright infringement cases against Sinovel Wind Group Co, Ltd (Sinovel) and Guotong Electric. During the proceedings, the court is expected to review the jurisdiction of AMSC's civil action filed against Sinovel in the Beijing No. 1 Intermediate People's Court as well as AMSC's civil action filed against Sinovel and Guotong Electric in the Hainan Province No. 1 Intermediate People's Court.

These are two of the four legal cases that AMSC brought against Sinovel in late 2011 regarding Sinovel's contractual breaches and AMSC's discovery of intellectual property theft by Sinovel. AMSC is also engaged in a commercial arbitration case and a trade secrets case against Sinovel in China.

(Continued above)

In September 2011, AMSC filed a civil action with the Beijing No. 1 Intermediate People's Court that alleges Sinovel's unauthorized copying and use of portions of AMSC's wind turbine control software developed for Sinovel's 1.5 MW wind turbines and the binary code, or upper layer, of AMSC's software for its PM3000 power converters. In this case, AMSC is seeking a cease and desist order and damages totaling US$6 million. In November 2011, Sinovel filed a motion to remove this case from the Beijing No. 1 Intermediate People's Court and transfer the matter to the Beijing Arbitration Commission.

The court denied Sinovel's motion to remove the case. Sinovel filed an appeal of that decision to the Beijing Higher People's Court, and the Beijing Higher People's Court supported the Beijing No. 1 Intermediate People's Court's ruling and rejected Sinovel's appeal. Sinovel then filed an appeal of that decision with China's Supreme People's Court.

In September 2011, AMSC also filed a copyright case against Sinovel and Guotong Electric with the Hainan Province No. 1 Intermediate People's Court. In this case, AMSC is seeking a cease and desist order as well as damages totaling approximately US$200,000, making this the smallest of AMSC's legal actions against Sinovel. In this case, Sinovel filed a jurisdiction opposition motion in December 2011 requesting that the Hainan Province No. 1 Intermediate People's Court dismiss AMSC's case against Sinovel, saying the case should be governed by the Beijing Arbitration Commission pursuant to the terms of component contracts between AMSC and Sinovel. Not only did the court grant Sinovel's motion, but also it dismissed the cases against both Sinovel and Guotong.

AMSC appealed the dismissal to the Hainan Higher Court, which on April 5, 2012 upheld the decision of the Hainan Province No. 1 Intermediate People's Court. AMSC then filed an appeal of that decision with China's Supreme People's Court.

"President Xi Jinping recently said that China would protect legitimate rights of foreign enterprises. AMSC's cases against Sinovel are the perfect litmus test for whether statements like these are rhetoric or reality. They will help to determine whether China will protect the intellectual property rights of all companies -- both foreign and domestic," said John Powell, Vice President and General Counsel, AMSC.

Congress Curtails Government IT Purchases from China

INFOWEEK GOVERNMENT
March 26, 2013

The continuing resolution funding the federal government through the end of September, which is now sitting on the President's desk and ready for his signature, bars government purchases of IT equipment produced by Chinese government-owned or -subsidized companies without prior consultation with the FBI. The bill reflects continued and rising concerns about Chinese hacking and other risks of Chinese technology. The Obama Administration recently has picked up rhetoric about Chinese hacking as reports continue to pour in about the Chinese government's connection to cyber espionage.

Specifically, the bill prohibits a short list of specific government agencies, including the Departments of Commerce and Justice, NASA and the National Science Foundation, from using funds made available as part of the continuing resolution to buy any IT unless the FBI "or other appropriate federal entity" has assessed the risk of "cyber-espionage or sabotage" that derives from the equipment being produced in connection with the Chinese government.

In addition, the law prohibits those agencies from using funds to buy IT systems produced, manufactured or assembled by companies or other entities owned, directed or subsidized by the Chinese government unless the head of the FBI or whatever agency is doing the assessment has both determined and reported to Congress that the acquisition is "in the national interest of the United States.

To review the rest of the article please click on the link:
http://www.informationweek.com/government/security/congress-curtails-government-it-purchase/240151739

Three N.Y.U. Scientists Accepted Bribes from China, U.S. Says

THE NEW YORK TIMES
May 20, 2013

It was, the chief federal prosecutor in Manhattan said on Monday, "a case of inviting and paying for foxes in the henhouse." Three researchers at the New York University School of Medicine who specialized in magnetic resonance imaging technology had been working on research sponsored by a grant from the National Institutes of Health. But, prosecutors charged on Monday, the three had their eyes on other business as well. They conspired to take bribes from a Chinese medical imaging company and a Chinese-sponsored research institute to share nonpublic information about their N.Y.U. work, according to the United States attorney's office in Manhattan.

The defendants, all Chinese citizens, included Yudong Zhu, 44, of Scarsdale, N.Y., an associate professor in the school's radiology department who was described by the authorities as "an accomplished researcher and innovator." He was hired by the university around 2008 to teach and conduct research related to innovations in M.R.I. technology, the authorities said.

After the National Institutes of Health awarded the university millions of dollars over five years to pay for Professor Zhu's research, he arranged for the two other defendants to move to New York from China to work with him, prosecutors said. He also arranged for them to receive financial support from an executive of the Chinese imaging company who was also affiliated with the government-sponsored institute, officials said.

The two other defendants are Xing Yang, 31, and Ye Li, also 31, both of Hartsdale, N.Y. They were each described by N.Y.U. as research engineers at the medical school. The support they received included graduate school tuition for Mr. Yang, a rental apartment for Mr. Li and, for both, travel between China and New York, prosecutors said.

Preet Bharara, the United States attorney, who announced the charges with George Venizelos, the head of the Federal Bureau of Investigation's New York office, said the defendants had "colluded with representatives from a Chinese government entity and a direct competitor of the university for which they worked to illegally acquire N.I.H.-funded research for the benefit of those entities." N.Y.U. said in a statement that it was "deeply disappointed by the news of the alleged conduct by its employees."

"Through our internal review processes," it said, "we became aware of possible irregularities pursuant to research being conducted through a grant from the N.I.H. to develop new M.R.I. technologies." The university said that it had alerted the authorities and continued to cooperate fully with the investigation.

Dr. Zhu and Mr. Yang were both arrested on Sunday and ordered released on bond by a magistrate judge on Monday. All three defendants were charged with one count of commercial bribery conspiracy; Dr. Zhu was also charged with one count of falsification of records. A prosecutor said in court that Dr. Zhu had admitted to the F.B.I. that he had received almost $500,000 in the scheme.

Dr. Zhu's lawyer, Robert M. Baum, said in court that N.Y.U. had recruited his client because he was "one of the world's renowned experts in M.R.I. technology. Mr. Li was believed to have flown to China before charges were brought, Mr. Bharara's office said.

Ex-GM Engineer's Husband Gets 3 Years for Secrets Theft

BLOOMBERG
May 1, 2013

A former General Motors Co. (GM) engineer's husband was sentenced to three years in prison for stealing hybrid technology trade secrets from the carmaker to help develop vehicles in China.

(Continued above)

Yu Qin, the husband of the ex-GM employee, was accused of using the Detroit-based carmaker's data to seek business ventures or employment with its competitors, including China's Chery Automobile Co. His wife, Shanshan Du, who will also be sentenced today, was accused of copying GM's private information on the motor control of hybrids and providing documents to her husband. "This is an extremely serious case involving a serious crime," U.S. District Judge Marianne O. Battani said at the sentencing hearing in federal court in Detroit today. "It is a crime in which our whole community, our whole economic structure is a victim."

Qin was convicted in November of three counts of trade secrets theft, three of wire fraud and one of obstruction of justice. Du was convicted on three trade-secret counts.
"This is all my fault," Qin said at the hearing. "I want to take full responsibility. I want to apologize to the court for all the trouble I caused." The secrets at issue were worth more than $40 million to General Motors, prosecutors said in a pre-sentencing memorandum filed last week. The U.S. asked Battani to sentence Qin and Du to as long as 10 years and a month in prison.

The defendants, who had pleaded not guilty, said the information didn't consist of trade secrets, wasn't stolen and was useless for other companies. They sought probation.

The case is one of more than a dozen brought in the past three years by the U.S. Justice Department alleging defendants of Chinese ancestry or citizenship sought to take trade secrets from U.S.-based companies for use by the Chinese government or businesses. Qin and Du are both U.S. citizens.

The case is U.S. v. Qin, 10-cr-20454, U.S. District Court, Eastern District of Michigan (Detroit).

Medical College of Wisconsin Researcher Charged with Economic Espionage

JSONLINE.COM
April 1, 2013

A researcher at the Medical College of Wisconsin has been charged with stealing a possible cancer-fighting compound and research data that led to its development, all to benefit a Chinese university. Huajun Zhao, 42, faces a single count of economic espionage, according to a federal criminal complaint, an offense punishable by up to 15 years in prison and a $500,000 fine. Zhao was arrested Saturday and held without bail over the weekend pending a detention hearing in Milwaukee federal court on Monday, when he was ordered detained until trial. No date has been set.

John Raymond, president and CEO of the Medical College of Wisconsin in Wauwatosa, said the school is cooperating with the FBI, and directed all other questions to the FBI. According to the complaint, Zhao worked as an associate researcher at the college, assisting-professor Marshall Anderson by conducting experiments in pharmacology.

To review the rest of the article please click on the link: http://www.bloomberg.com/news/2013-04-02/wisconsin-cancer-researcher-accused-of-economic-spying-for-china.html?cmpid=

Former Employee of New Jersey Defense Contractor Sentenced to 70 Months in Prison for Exporting Sensitive Military Technology to China

U.S. DEPARTMENT of JUSTICE
PRESS RELEASE
March 25, 2013

A former New Jersey-based defense contractor employee – who was convicted by a federal jury for exporting sensitive US military technology to the People's Republic of China (PRC), stealing trade secrets and lying to federal agents – was sentenced in March to 70 months in prison, New Jersey US Attorney Paul J. Fishman announced. Sixing Liu, a/k/a, —Steve Liu, 49, a PRC citizen who had recently lived in Flanders, N.J., and Deerfield, Ill., has been in custody since the September 2012 verdict, based on his risk of flight.

Instead of the accolades he sought from China, Sixing Liu today received the appropriate reward for his threat to our national security: 70 months in prison, said US Attorney Fishman. As an innovation leader, the United States is a target for those seeking to cut corners at the expense of American businesses and consumers. As this sentence shows, the Department of Justice is making great progress in the fight against trade secret theft in order to protect the engines of our nation's economic recovery.

The jury convicted Liu of nine of the 11 counts in the Second Superseding Indictment with which he was charged, including six counts of violating the Arms Export Control Act and the International Traffic in Arms Regulations, one count of possessing stolen trade secrets in violation of the Economic Espionage Act of 1996, one count of transporting stolen property in interstate commerce and one count of lying to federal agents. In addition to the prison term, Liu was sentenced to serve three years of supervised release and ordered to pay a $15,000 fine. Restitution is to be determined at a later date.

According to documents filed in the case and evidence presented at trial: In 2010, Liu stole thousands of electronic files from his employer, L-3 Communications, Space and Navigation Division, located in Budd Lake, N.J. The stolen files detailed the performance and design of guidance systems for missiles, rockets, target locators and unmanned aerial vehicles. Liu stole the files to position and prepare himself for future employment in the PRC. As part of that plan, Liu delivered presentations about the technology at several PRC universities, the Chinese Academy of Sciences and conferences organized by PRC government entities.

(Continued below)

On Nov. 12, 2010, Liu boarded a flight from Newark Liberty International Airport to the PRC. Upon his return to the United States on Nov. 29, 2010, agents found Liu in possession of a non-work-issued computer containing the stolen material. The following day, Liu lied to agents of the Department of Homeland Security about the extent of his work on US defense technology, which the jury found to be a criminal false statement.

The US Department of State's Directorate of Defense Trade Controls later verified that several of the stolen files on Liu's computer contained export-controlled technical data that relates to defense items listed on the United States Munitions List (USML). Under federal regulations, items and data covered by the USML may not be exported without a license, which Liu did not obtain.

The regulations also provide that it is the policy of the United States to deny licenses to export items and data covered by the USML to countries with which the United States maintains an arms embargo, including the PRC. The jury heard testimony that Liu's company trained him about the United States' export control laws and told him that most of the company's products were covered by those laws.

US Attorney Fishman credited special agents of the FBI, under the direction of Acting Special Agent in Charge David Velazquez; special agents of ICE-Homeland Security Investigations, under the direction of Special Agent in Charge Andrew McLees; and officers of US Customs and Border Protection, under the leadership of Director of New York Field Operations Robert E. Perez, for the investigation leading to the sentence.

Flash Player Click-Jacking Flaw Allows Hackers to Hijack your Webcam

SOFTPEDIA
June 14, 2013

A researcher discovered vulnerability in Adobe's Flash Player that can be exploited to access a user's webcam and microphone if the user is using the Mac version of Chrome, Linux, Chromium, and possibly other configurations.

Digital Cameras Easily Turned into Spying Devices, Researchers Prove

HELPNET SECURITY
March 25, 2013

Users' desire to share things online has influenced many markets, including the digital camera one. Newer cameras increasingly sport built-in Wi-Fi capabilities or allow users to add SD cards to achieve them in order to be able to upload and share photos and videos as soon as they take them. But, as proven by Daniel Mende and Pascal Turbing, security researchers with German-based IT consulting firm ERNW, these capabilities also have security flaws that can be easily exploited for turning these cameras into spying devices.

Mende and Turbing chose to compromise Canon's EOS-1D X DSLR camera an exploit each of the four ways it can communicate with a network. Not only have they been able to hijack the information sent from the camera, but have also managed to gain complete control of it.

To review the rest of the article click on the link: http://www.net-security.org/secworld.php?id=14651

What Is Email Spoofing All About?

MIT NEWS
May 6, 2013

You've been receiving emails from a friend recently telling you about some "amazing" information with a link that seemingly leads nowhere. When you ask her about the emails, she tells you she didn't send them. Why is this happening? It's probably a case of email spoofing. Email spoofing, used in a large portion of spam, is a modern form of forgery where certain email information is masked in an attempt to trick the recipient into believing the message came from someone else.

(Continued below)

Spoofed emails are designed to elicit a certain behavior from you, the email recipient. The goal could be for you to click on a link leading to a website containing malware, to open a virus-laden attachment, or to reply with information that is personal or confidential. A common way spammers trick you is by using the name of a friend or someone you know in the "From:" field and as the signature. Fraudulent messages often contain urgent requests such as: "Your email account has been suspended," "Help, I'm stuck abroad and need money," or "Please open this invoice." The tactics are nearly endless, but the goal is always the same: to try, through social engineering, to get you to complete an action. After all, you trust your friends. Right?

Not so fast. If you look closely, the "From:" email address is not legitimate, even though the name that appears before it may be. Look also at the email's full headers. You can use these headers to verify the original source of the message. In a legitimate email, the return path (the email address the message was really sent from) will usually match the address that appears in the email's "From:" field. A fraudulent email will show a different address as the return path. In most spoofed email, the "Reply-To:" address in the email will also be different.

Spammers get names and addresses through compromised email accounts, which give them access to contact lists. If a friend has his or her email account compromised, then you may become a target for spoofed email. Information about relationships can also be obtained from social network profiles that are public or have weak privacy settings.

Because there's no effective way to stop spammers from spoofing, there's generally nothing you can do about these messages except to delete them. Luckily, spammers tend to abandon address books quickly, moving on to other lists and new targets.

To review the rest of the article please click on the link:
http://web.mit.edu/newsoffice/2013/email-spoofing-whats-it-all-about.html

NetTraveler Spyware Compromised 1,000 Political and Industrial Targets

INFOSECURITY
June 4, 2013

The malware behind a widespread cyber-espionage campaign against political and critical industry targets has been called out: NetTraveler, a malicious program used for covert computer surveillance, has successfully compromised at least 350 high-profile victims in 40 countries, with the total likely closer to 1,000.According to sinkhole analysis from Kaspersky Lab, the campaign is being carried out by an organized group. "We estimate the group size to about 50 individuals, most of which speak Chinese natively and have working knowledge of the English language," it said.

The bug is part of an advanced persistent threat (APT) campaign, used for basic surveillance of the victims. It's designed to steal sensitive data as well as log keystrokes, and retrieve file system listings and various Microsoft Office or PDF documents. Known targets of NetTraveler (also known as Travnet or Netfile) include Tibetan/Uyghur activists, oil industry companies, scientific research centers and institutes, universities, private companies, governments and governmental institutions, embassies and military contractors.

To review the rest of the article please click on the link:
http://www.infosecurity-us.com/view/32755/nettraveler-spyware-compromised-1000-political-and-industrial-targets/

Chinese Military Unit Said to Resume Cyber Spying

TRIBUNE WASHINGTON BUREAU
May 16, 2013

A Chinese military unit that a private U.S. computer security company accused of launching more than 115 cyber attacks against American companies over seven years has resumed hacking after a three-month hiatus, the company's chief security officer said Wednesday.

(Continued below)

The clandestine army unit, known as Unit 61398, "went quiet for a while—they changed the nature of their activities, they removed some of the tools that they had been using inside of different companies," said Richard Bejtlich of Mandiant, which specializes in defending companies from cyber attacks and purging malware from computer networks that have been breached.

"But over the course of the last several weeks it seems they are trying to ramp back up.... They seem to be trying to get back into some of their old targets," he said.

Bejtlich's remarks to the Center for National Policy, a nonpartisan think tank in Washington, came as the Obama administration weighs how to respond to what senior officials have called a massive campaign of commercial espionage emanating from China, and as Congress mulls legislation to enable companies and the government to share cyber-threat information.

China disputes that it engages in commercial espionage through hacking, but Bejtlich and other private researchers, backed by U.S officials, say breaches of U.S. corporate networks from China have not tapered off. The U.S. government makes aggressive use of cyber spying, including against China, but officials say it does not target economic secrets for the benefit of American industry.

On Tuesday, Gen. Keith Alexander, who heads the National Security Agency and U.S. Cyber Command, told a cyber-security summit sponsored by the Reuters news agency that U.S. computer networks are under constant attack, in some cases by those seeking to steal valuable corporate secrets and in other cases by adversaries bent on disrupting or destroying networks.

"Mark my words, it's going to get worse," Alexander said, according to Reuters. "The disruptive and destructive attacks on our country will get worse and ... if we don't do something, the theft of intellectual property will get worse."

(Continued above)

Mandiant's report in February marked the first public airing of detailed evidence linking the Chinese military to a huge cyber-theft campaign. The Los Angeles Times later reported 2007 blog posts by a 25-year-old member of the military unit who boasted of perfecting a tool to infiltrate computer networks that escaped detection by leading antivirus software.

Mandiant did not identify the companies targeted by Unit 61398, citing confidentiality agreements with its clients. Bejtlich did not say Wednesday where the unit has resumed its attacks, but he said other China-based groups never stopped stealing Western intellectual property.

"They steal a staggering amount of information," he said.
Bejtlich said the U.S. government should take action against China to force it to crack down on the thefts.
"We've been talking with them for a long time about this ... and they have not stopped," he said.

Chinese University Lab Linked to PLA Cyber Attacks

FREEBEACON
May 14, 2013

A computer science laboratory at China's Wuhan University has been linked by U.S. intelligence agencies to Chinese military cyber attacks on the West. According to U.S. officials, the Key Laboratory of Aerospace Information Security and Trusted Computing at Wuhan's Computer Science School in central China's Hubei Province is the latest cyber warfare research and attack center to be identified from within China's secret cyber warfare program.

The Pentagon's latest annual report on China's military, made public last week, for the first time confirmed that Chinese cyber attacks on the U.S. government appeared "attributable directly to the Chinese government and military." A report by the private cyber security firm Mandiant in February identified China's main military cyber espionage group near Shanghai as Unit 61398, part of the People's Liberation Army's 2nd Bureau of the General Staff Department's 3rd Department, known as 3PLA. According to U.S. officials, the Key Laboratory, located about 425 miles west of the Chinese port city of Shanghai, is one of three computer science laboratories at the university.

(Continued below)

It was set up in 2008 and is considered one of the premier information security and cyber warfare centers at the university.

To review the rest of the article please click on the link: http://freebeacon.com/network-effects/?print=1

Robust Spending on Cyber Warfare Systems until 2023

**Modern Society's Growing Dependence on Technological Infrastructure, and the Ever-Changing Nature of Cyber-threats, Will Fuel Continued Growth of the Cyber security Market Over The Next Decade*

With the increasing importance of information and communication technologies both on and off the battlefield, new research available on ASDReports forecasts continued robust global spending on cyber warfare systems until 2023, with the market expanding from US$11.1 billion in 2013 to US$19.4 billion by 2023 – a CAGR of 5.77%. This significant growth is further fuelled by a surge in the number of cyber attacks, the pressure of austerity measures on Western defense budgets, and the relentless advancement in cyber crime technologies.

North America Is Expect to Lead the Global Cyber-security Market

The US is the largest defense spender in the world, so perhaps unsurprisingly dominates the global cyber security market – research indicates that it will spend US$93.5 billion on cyber security between 2013 and 2023, representing a 56% share of the global market.

Whilst Europe has borne the brunt of the global economic crisis, which has had a detrimental effect on military spending, the region is still expected to increase its cyber warfare systems spending over the next decade, though will be overtaken by the ever more powerful Asia Pacific region, which is expected to hold the second largest share of the cyber security market – 14% - by 2023.

(Continued above)

Cyber warfare is yet to be wholeheartedly adopted by South American countries, but Brazil, Mexico, Colombia, Venezuela and Chile are expected to be the key spenders in the region over the next ten years, as they seek to defend their country's networks from increasingly organized cyber attacks.

Increased Dependence on Information Technology Resulting in More Cyber Attacks

Modernised living – from infrastructure to banking, defense, and energy production – is inextricably linked to the computing power of a nation. Whilst these computer systems have resulted in a highly effective ecosystem, the pervasive use of technology has also given rise to great vulnerability, with society's dependence on technology leaving the most important aspects of daily life open to attack.

It is not only the civil domain that is becoming increasingly dependent on information technology: according to William J. Lynn, former US Deputy Secretary of Defense, the command and control of the US' forces, intelligence, logistics, and weapons technology all depend on 15,000 US networks connecting 7 million computers, information technology devices and servers – all of which are at risk from cyber attacks.

Adding to this vulnerability is the fact that cyber attacks are now not only limited to nations, but have extended to terrorist groups, organized crime, hackers, industrial spies, and foreign intelligence services.

Fear regarding attacks on increasingly vital technological infrastructure is one of the primary drivers fuelling growth in the global cyber security market. Whilst historically, most of the expenditure in the cyber security market is generated by the private sector, Strategic Defense Intelligence's research reveals that government spending has witnessed a robust recent increase: the US' private and public sector spending is almost the same, whilst the UK has made cyber security a 'tier one priority', allocating an additional US$800 million for cyber security initiatives in its 2010 strategic defense and security review, with the government expected to spend close to US$6 billion on cyber security over the next 10 years.

(Continued below)

Dynamic Nature of Cyber Threats Warrants Increased Spending on Innovative Technologies

Although many countries worldwide are cutting their defense budgets, cyber warfare spending is set to increase significantly. In part, this can be attributed to the novelty of the market, with governments and private organizations seeking to stay ahead of the ever-changing curve.

This novelty means that sufficient countermeasures have historically not always been able to keep up with the rapid pace at which potential threats are developed, and so cutting edge cyber security is high on the global agenda. These ever changing dynamics of cyber threats, along with the increased demand for cyber weapons, has been identified as a primary growth driver over the next decade.

Read more: http://www.asdnews.com/news-49710/Robust_Spending_on_Cyber_Warfare_Systems_until_2023.htm?HASH=c8f69915b03274a709972e2947c2767d&utm_source=ASDNews&utm_medium=email&utm_campaign=ASDNews+Daily+Z1&utm_content=jeanette%40eib.com#ixzz2Wg8LKGSP