EIB World Trade Headlines

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

July 1, 2016 - Volume 8, Issue 12

Venezuela Is About to Explode

Last year, 8-year-old Oliver Sanchez became the poster child of the nightmare that is now Venezuela. He had non-Hodgkin's lymphoma and was in severe danger because hospitals and medicine banks had run out of supplies. Countless sick and desperate Venezuelan patients and family members looked to him with hope as he bravely protested in the streets with a handmade sign that read, "I want a cure, peace and health." The media and public rallied around Oliver, posting photos of him on social media, begging the government to do something.

On May 26, Oliver died. He reportedly contracted meningitis and, due to medicine shortages, succumbed to the infection. Oliver's death spread a wave of rage among Venezuelans. Opposition lawmakers held up pictures of the boy to decry what they called an avoidable death. And yet, the people and Oliver's family have heard not a word from the government. The silence is deafening.

Venezuela has the highest inflation rate and the second highest murder rate in the world and a scarcity of basic goods and medicine only conceivable during war. But there hasn't been a war in Venezuela, or even a natural disaster.

*(*Continued On The Following Page)*

NEWSLETTER NOTES

***Venezuela Is About to Explode**

***CT Industries to benefit from NDAA**

***Homeland Security National…**

***CHIEF EXECUTIVE OFFICER OF…**

***NEW JERSEY MAN PLEADS GUILTY TO…**

***Joint Summary of Outcomes**

***Six Airlines, Five US Cities Chosen…**

***Russian government hackers penetrated…**

***Bombardier CS100 Aircraft…**

***The Government of Iraq…**

***Carrier says it will acquire planes…**

***Modine Manufacturing…**

***Addition of Certain…**

What led to such a crisis? It's a complex story of excess, megalomania and hate. Moises Naim and Francisco Toro write brilliantly how the country fell apart during 17 years of rule by Hugo Chavez and and his hand-picked successor, Nicolas Maduro. The images tell the story: long lines of humiliated citizens, with numbers marked by soldiers on their arms, trying to buy subsidized food so scarce that it's sold for 10 to 20 times its price on the black market. Increasing numbers of people, unable to buy food, are resorting to scavenging in the trash, fighting police and looting grocery stores.

In this beautiful corner of the Caribbean, electricity is rationed, so government employees work just two days a week; water is severely polluted; people leave the few jobs that are left to search for food or to work on the black market. Several thousand companies have closed. The schools are being deserted because teachers must look for groceries as well and children are often used by families to keep places in long lines.

The difficulties to produce or import food remain unchanged, so scarcity hardens every week, as does inflation. Once you gather the money to buy, say, a kilogram of chicken — which could be a month's earnings at minimum wage — you might find that the price increased dramatically overnight.


RONALDO SCHEMIDT via Getty Images

However, Maduro hasn't employed available measures to turn the economy around the corner.

He prefers the advice of his Marxist advisor from Spain to the businessman chosen as minister of economy. He keeps saying that the crisis is a conspiracy and blames everything, even crime, on the opposition. In response to unrest, he declared a state of emergency, allowing police and military to arrest or shoot anyone.

The government's strategy, as far as one can infer from its actions, is to resist and wait for higher oil prices or a new big loan from China. To maintain order, Maduro seems to rely on the Electoral Council, the Supreme Court and the weapons of those who support him: the military, paramilitary and police, which are deeply involved in smuggling, drug dealing and kidnapping.

An opposition alliance won parliamentary elections last December but it can't make any new laws effective. The Supreme Court, controlled by Maduro, declares unconstitutional everything that the National Assembly does. Isolated as a power with zero influence aside from its popularity, the opposition looks for ways to break the *Chavista* hegemony over Venezuela's institutions.

*(*Continued On The Following Column)*

Part of the opposition, led by popular governor Henrique Capriles, demands a recall referendum against Maduro. According to the constitution, if Maduro is recalled in 2016, a general election should follow and Capriles can run for office — for the third time. If the referendum happens in 2017 and Maduro loses it, his vice president becomes president until 2019, so *Chavismo* would stay in power. A recall next year is the preferred scenario for those *Chavistas* who are against Maduro and for those within the opposition who don't want Capriles as president.

Polls say a recall is what millions hope for. People need change, and they need it now. But Maduro continues to pressure the Electoral Council, which ignores its own rules to boycott efforts toward a referendum. Meanwhile, the opposition cries for help from neighboring countries.

The secretary general of the Organization of American States, Luis Almagro, requested an emergency meeting to consider expelling Venezuela, saying that "grave alterations of democratic order" had been committed by the government. But thanks to some surprising help from Argentina's new right-leaning government, the effort has stumbled.

The Maduro regime recently added another terrible idea to its defensive tactics: forbidding stores to sell subsidized groceries and creating Soviet-style committees called CLAPs to deliver them directly to the people. Not to everyone, though: CLAPs give food only to Maduro's supporters or sell it on the black market.

The consensus among many Venezuelans these days is that something big is going to happen, and it will be bad.

People's worries aren't nonsensical. None of the political actors can control the outcome of this crisis — not even Maduro, who is despised among some *Chavista* factions that can't restrain him. There are no referees; public institutions lost independence years ago, and *Chavismo* doesn't respect the Catholic Church or intellectuals. Nobody trusts anyone. *Chavistas* around the president probably fear a wave of revenge if they're ousted.

If the proposed OAS dialogue fails and the recall referendum is postponed, can tensions push Venezuela into a civil war for the first time since the 1860s? The opposition has neither the means nor the will to build a rebel army. What about a coup d'état? This is more probable but nobody knows for sure who's against whom in an army with lots of privileges, where dissent is severely punished. The generals display nothing but loyalty to the political movement that brought them back to influence after 40 years of civilian presidents.

(*Continued On The Following Page)

The most likely scenario is the most terrifying: generalized looting. Will the police and the army shoot the mob, like they did during the 1989 revolt, years before the ascent of Chavez? Or will they accompany Venezuelans in a rampage for survival? The word is that some units won't follow Maduro's orders to kill in such a situation.

Only two bottles of cooking oil remain on the shelf at a government grocery store in Caracas on Jan. 27, 2016. (Meridith Kohut/Bloomberg via Getty Images)

Uncontrolled violence would benefit the strongest in a country that has turned into a crime sanctuary. Powerful gangs target police. They have assault rifles and grenades, they rule over jails and entire towns, they hijack boats at sea. They would dominate looting and resell stolen goods. And Venezuela could end up as a completely failed state — a Somalia in the Caribbean.

Fantasy? Not quite: there's already a lynching epidemic, and at least one person accused of robbery was burned alive. The breaking of what's left of social cohesion could be around the corner.

Everybody feels that something big can happen any time. Those who can are trying to prepare for the worst. Ordinary people are just trying to survive day by day. Some of them manage. Others don't.

CT Industries to benefit from NDAA

National Defense Authorization Act for Fiscal Year 2017 passed on Tuesday authorizes funding for:
•$5 billion for two Virginia Class submarines
•$1.5 billion for Ohio Replacement Program submarines
•$8.5 billion for 63 Joint Strike Fighters
•$929 million for 36 Black Hawk helicopters
•$437 million for 2 Marine Corps' CH-53K helicopters
•$61 million for the Navy MH-60R Naval Hawk helicopter program
•$302 million UH-1N helicopters replacement helicopter program
•$6.3 million for the Small Air Terminal at Bradley International Airport for the Connecticut National Guard

Homeland Security National Terrorism Advisory System Bulletin

Date Issued: Wednesday, June 15, 2016
View as PDF: National Terrorism Advisory System Bulletin - June 15, 2016 (pdf, 1 page, 876.65KB)

Summary

In December, we described a new phase in the global threat environment, which has implications on the homeland. This basic assessment has not changed. In this environment, we are particularly concerned about homegrown violent extremists who could strike with little or no notice. The tragic events of Orlando several days ago reinforce this. Accordingly, increased public vigilance and awareness continue to be of utmost importance. This bulletin has a five-month duration and will expire just before the holiday season. We will reassess the threats of terrorism at that time.

Duration

Issued: June 15, 2016
Expires: November 15, 2016

Details

- Since issuing the first Bulletin in December, our concerns that violent extremists could be inspired to conduct attacks inside the U.S. have not diminished.
- Though we know of no intelligence that is both specific and credible at this time of a plot by terrorist organizations to attack the homeland, the reality is terrorist-inspired individuals have conducted, or attempted to conduct, attacks in the United States.
- DHS is especially concerned that terrorist-inspired individuals and homegrown violent extremists may be encouraged or inspired to target public events or places.
- As we saw in the attacks in San Bernardino, Paris, Brussels, and, most recently, Orlando, terrorists will consider a diverse and wide selection of targets for attacks.
- Terrorist use of the Internet to inspire individuals to violence or join their ranks remains a major source of concern.

In the current environment, DHS is also concerned about threats and violence directed at particular communities and individuals across the country, based on perceived religion, ethnicity, nationality or sexual orientation.

*(*Continued On The Following Page)*

U.S. Government Counterterrorism Efforts

- DHS and the FBI continue to provide guidance to state and local partners on increased security measures. The public may observe an increased law enforcement and security presence across communities, in public places and at events in the months ahead. This may include additional restrictions and searches on bags, more K-9 teams, and the use of screening technologies.
- The FBI is investigating potential terrorism-related activities associated with this broad threat throughout the United States. Federal, state, and local authorities are coordinating numerous law enforcement actions and conducting community outreach to address this evolving threat.

Types of Advisories

- Bulletin
- Describes current developments or general trends regarding threats of terrorism.
- Elevated Alert
- Warns of a credible terrorism threat against the United States.
- Imminent Alert
- Warns of a credible, specific and impending terrorism threat against the United States.

How You Can Help

- Report suspicious activity to local law enforcement or public safety officials who are best positioned to respond and offer specific details on terroristic indicators.
- Suspicious activity or information about a threat may also be reported to Fusion Centers and the FBI's Field Offices - part of the Nationwide Suspicious Activity Reporting Initiative.
- Learn how to recognize signs of pre-operational planning associated with terrorism or other criminal activity.

Be Prepared

- Be prepared for increased security and plan ahead to anticipate delays and restricted/prohibited items.
- In populated places, be responsible for your personal safety. Make a mental note of emergency exits and locations of the nearest security personnel. Keep cell phones in your pockets instead of bags or on tables so you don't lose them during an incident. Carry emergency contact details and any special needs information with you at all times. For more visit Ready.

*(*Continued On The Following Column)*

Stay Informed

- The U.S. Government will provide additional information about any emerging threat as additional information is identified. The public is encouraged to listen to local law enforcement and public safety officials.
- We urge Americans to continue to travel, attend public events, and freely associate with others but remain vigilant and aware of surroundings.
- The Department of State issues international travel alerts and warnings.

If You See Something, Say Something™. Report suspicious activity to local law enforcement or call 911.

The National Terrorism Advisory System provides Americans with alert information on homeland security threats. It is distributed by the Department of Homeland Security. More information is available at: www.dhs.gov/advisories. To receive mobile updates: twitter.com/dhsgov

CHIEF EXECUTIVE OFFICER OF INTERNATIONAL METALLURGICAL COMPANY PLEADS GUILTY TO CONSPIRING TO EXPORT SPECIALTY METALS TO IRAN

Earlier today in federal court in Brooklyn, Erdal Kuyumcu, the chief executive officer of Global Metallurgy, LLC, a company based in Woodside, New York, pleaded guilty to one count of conspiring to violate the International Emergency Economic Powers Act in connection with the export of specialty metals from the United States to Iran. Today's plea proceeding took place before Chief United States District Judge Dora L. Irizarry. The guilty plea was announced by Robert L. Capers, United States Attorney for the Eastern District of New York, and John P. Carlin, Assistant Attorney General for National Security. As detailed in the criminal information to which he pleaded guilty and in related court filings, Kuyumcu, a United States citizen, conspired to export from the United States to Iran a metallic powder composed of cobalt and nickel without having obtained the required license from the U.S. Treasury Department's Office of Foreign Assets Control (OFAC). The metallic powder can be used to coat gas turbine components, such as turbine blades, and can also be used in aerospace, missile production, and nuclear applications. Such specialized metals are closely regulated by the U.S. Department of Commerce to combat nuclear proliferation and protect national security, and exporting them without an OFAC license is illegal. Kuyumcu and others conspired to obtain over one thousand pounds of the metallic powder from a U.S.-based supplier for export to Iran. To hide the true destination of the

(*Continued On The Following Page)

from the U.S. supplier, Kuyumcu and a co-conspirator arranged for the metallic powder to be shipped first to Turkey and then to Iran.

In announcing the guilty plea, Mr. Capers extended his grateful appreciation to the Federal Bureau of Investigation, New York Field Office, and the U.S. Department of Commerce, Bureau of Industry and Security, Office of Export Enforcement, New York Field Office, the agencies that led the government's investigation.2

At sentencing, Kuyumcu faces up to 20 years in prison a $1 million fine.

The case is being prosecuted by Assistant U.S. Attorneys Tiana A. Demas and Ameet B. Kabrawala of the Eastern District of New York, with assistance from Trial Attorney David Recker of the National Security Division's Counterintelligence and Export Control Section.

The Defendant:
ERDAL KUYUMCU
Age: 44
Woodside, New York
E.D.N.Y. Docket No. 16-CR-308 (DLI)

NEW JERSEY MAN PLEADS GUILTY TO CONSPIRACY TO PROVIDE FALSE STATEMENTS RELATED TO EXPORT OF PROHIBITED GOODS TO IRAN

The United States Attorney's Office for the Middle District of Pennsylvania announced today that a New Jersey man pleaded guilty to conspiring to provide false statements related to illegally exporting goods to Iran before United States Magistrate Judge Joseph F. Saporito in Wilkes-Barre.

According to United States Attorney Peter Smith, Asim Fareed, age 51, of North Brunswick, New Jersey, pleaded guilty to conspiracy to provide false statements in connection to the illegal export of goods to Iran. According to the Information to which he pleaded guilty, Fareed operated an export business in Somerset, New Jersey and agreed to ship items purchased by customers in Iran and to provide false documentation to the U.S. Department of Commerce for export purposes. Communications concerning the shipments passed between New Jersey and a site in Lackawanna County, Pennsylvania. No actual shipments were, in fact, delivered to Iran.

The Information charges that in 2013 and 2014 Fareed conspired with others to export items from the United States, through third party countries to customers in Iran. According to the Information, Fareed prepared invoices which included false information as to the identity and geographic location of the purchasers of the goods. The items were then to be shipped from the United States to the United Arab Emirates, and thereafter transshipped to Iran. The guilty plea is pursuant to a plea agreement with the government.

*(*Continued On The Following Column)*

"The Office of Export Enforcement protects our national security and foreign policy interests by vigorously pursuing violators of our nation's export control laws. Today's guilty plea is an example of our close work with our colleagues at HSI and other law enforcement agencies to complement our robust enforcement program. Providing or causing false statements on export documents and illicit trade with Iran will remain a high priority for the Office of Export Enforcement," said Jonathan Carson, Special Agent in Charge, U.S. Department of Commerce, Bureau of Industry and Security, Office of Export Enforcement, New York Field Office."

"This case demonstrates how far individuals will go to circumvent U.S. export laws to export goods to countries like the Islamic Republic of Iran," said Angel M. Melendez, special agent in charge of HSI in New York. "The Iran Trade Embargo prohibits Americans from supplying goods, technology and services to Iran directly or indirectly. HSI is committed to aggressively pursuing those who conduct illegal business with Iran."

No sentencing date has been scheduled.

The case was investigated by the Department of Commerce, Office of Export Enforcement and U.S. Immigration and Custom Enforcement's (ICE), Homeland Security Investigations (HSI). Assistant U.S. Attorney Todd K. Hinkley is prosecuting the case.

A sentence following a finding of guilty is imposed by the Judge after consideration of the applicable federal sentencing statutes and the Federal Sentencing Guidelines.

Under the Federal Sentencing Guidelines, the Judge is also required to consider and weigh a number of factors, including the nature, circumstances and seriousness of the offense; the history and characteristics of the defendant; and the need to punish the defendant, protect the public and provide for the defendant's educational, vocational and medical needs. For these reasons, the statutory maximum penalty for the offense is not an accurate indicator of the potential sentence for a specific defendant.

CIVIL PENALTY INFLATION ADJUSTMENTS

The Department of State is implementing "catch-up" adjustments to the maximum amounts of the civil monetary penalties (CMPs) it assesses. The Department is making these adjustments because under the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015 (Section 701 of Pub. L. 114-74), Congress has mandated agencies to make a one time "catch-up" adjustment to their CMPs in order to account for inflation, which erodes the real value of statutorily mandated penalty amounts. The adjustment will be announced as a final rule on June 7, 2016. The 2015 Act also instructs agencies to make subsequent annual inflationary adjustments no later than January 15 of each year.

*(*Continued On The Following Page)*

Per the legislation, these updated CMP amounts will apply to all penalties assessed after August 1, 2016, regardless of when the actual violation(s) occurred. The methodology for catch-up adjustments was mandated by the legislation and distributed to agencies by the Office of Management and Budget (OMB) in OMB Memorandum M-16-06, dated February 24, 2016.

The CMP amounts assessed by the Directorate of Defense Trade Controls (DDTC) are included in the final rule. These CMP amounts authorized by the Arms Export Control Act ("AECA," 22 U.S.C. 2751 et seq.) will be adjusted as follows:

- For each violation of 22 U.S.C. 2778, an amount not to exceed $1,094,010 (previously $500,000);
- For each violation of 22 U.S.C. 2779a, an amount not to exceed $795,445 (previously $500,000); and
- For each violation of 22 U.S.C. 2780, an amount not to exceed $946,805 (previously $500,000).

While DDTC is making this required adjustment to the maximum amounts of CMPs it may assess, it is important to note that the 2015 Act does not impede the discretion of agencies to assess CMPs lower than the maximum amount should circumstances warrant.

Joint Summary of Outcomes

Today, Chinese State Councilor and Minister of Ministry of Public Security Guo Shengkun co-chaired the second U.S.-China Cybercrime and Related Issues High Level Joint Dialogue with representatives of the U.S. Departments of Justice and Homeland Security. The dialogue aims to implement the consensus reached between Chinese President Xi Jinping and U.S. President Barack Obama in September 2015 during President Xi's visit to the United States, and to enhance pragmatic bilateral cooperation with regard to cybercrime, network protection and other related issues.

Since the first dialogue, both sides have worked to implement the consensus reached between the two countries' presidents and the outcomes of the first dialogue. Both sides continue to develop cooperation on combating cybercrime and network protection investigations and information exchanges, aiming to conduct routine exchanges and improve cyber security cooperation.

The outcomes of the second dialogue are listed as below:

*(*Continued On The Following Column)*

Tabletop Exercise. Both sides value the cyber tabletop exercise held in April 2016, and regard the exercise as informative and effective. Both sides decided to hold a second tabletop exercise concerning cybercrime and network protection prior to the next dialogue.

Hotline Mechanism. Both sides decided to implement the "U.S.-China Cybercrime and Related Issues Hotline Mechanism Work Plan," and have reached consensus on the scope, objective and procedures of the hotline. China and the United States decided to test the hotline mechanism before September 2016.

Network Protection. Both sides decided to continue to strengthen cooperation in network protection. Both sides decided to hold a network security and protection working-level expert seminar in August 2016 in China. The experts decided to meet regularly in the future and report to the ministerial level at the High-Level dialogue in the future.

Information Sharing, Case Cooperation and Resources. Both sides decided to: enhance case investigations and information exchange related to cybercrime and other malicious cyber activities; exchange information and develop cooperation in cybercrime investigations and cyber incidents of mutual concern; hold a workshop to discuss how to enhance information exchanges and handling related to Mutual Legal Assistance Agreement (MLAA); and share cyber threat information on a regular basis, including increasing information sharing of malicious software samples and related analysis reports. Both sides acknowledge the importance of the increase of manpower and resources to tackle cybercrime threats and decided to further strengthen communication mechanisms as well as respective central authorities under the MLAA. Both sides discussed the 24/7 High Tech Network of international points of contact for the purpose of assisting in investigations involving electronic evidence that require urgent assistance from foreign law enforcement.

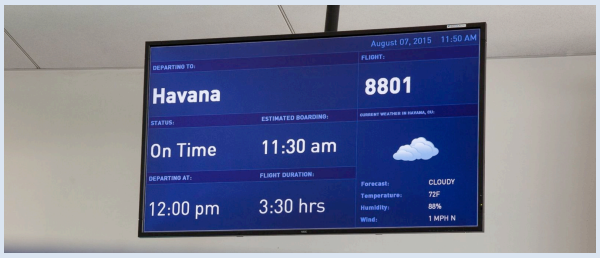
Cyber-Enabled Crime. Both sides commit to prioritize cooperation on combatting cyber-enabled intellectual property (IP) theft for commercial gain and cooperate in law enforcement operations in four additional areas: online child pornography distribution, misuse of technology and communications for terrorist activities, commercial email compromise/phishing and online firearms trafficking. Both sides decided to conduct a proposed seminar on misuse of technology and communications to facilitate violent acts of terrorism in 2016 in China before the next round of the dialogue. The United States and China decided to create an action plan to address the threat posed from business email compromise scams.

Senior Experts Group. Both sides discussed the first U.S.-China Senior Experts Group on International Norms in Cyberspace and Related Issues.

Third High-Level Dialogue. Both sides plan to hold the next round of the dialogue in the second half of 2016 in Washington, D.C.

Six Airlines, Five US Cities Chosen for Regular Service to Cuba

As the United States moves towards normalizing relations with Cuba, U.S. officials have announced the cities and airlines that will kick off regular commercial service between the countries for the first time in more than 50 years.



The carriers are American Airlines, Frontier Airlines, JetBlue Airways, Silver Airways, Southwest Airlines and Sun Country Airlines.

Flights could start departing for the Caribbean nation as soon as this fall from Miami, Fort Lauderdale, Chicago, Minneapolis/St. Paul and Philadelphia.

The Cuban cities selected are Camagüey, Cayo Coco, Cayo Largo, Cienfuegos, Holguín, Manzanillo, Matanzas, Santa Clara and Santiago de Cuba. Flights to Havana have not yet been approved, but officials said they are coming.

As part of the agreement, each country will have the chance to schedule up to 10 daily round-trip flights between the designated cities.

Long-term plans include flights to and from Havana and details on those trips will be announced later this summer, according to the U.S. Department of Transportation.

Russian government hackers penetrated DNC, stole opposition research on Trump

Russian government hackers penetrated the computer network of the Democratic National Committee and gained access to the entire database of opposition research on GOP presidential candidate Donald Trump, according to committee officials and security experts who responded to the breach.

The intruders so thoroughly compromised the DNC's system that they also were able to read all email and chat traffic, said DNC officials and the security experts.

The intrusion into the DNC was one of several targeting American political organizations. The networks of presidential

*(*Continued On The Following Column)*

candidates Hillary Clinton and Donald Trump were also targeted by Russian spies, as were the computers of some GOP political action committees, U.S. officials said. But details on those cases were not available.

A Russian Embassy spokesman said he had no knowledge of such intrusions.

Some of the hackers had access to the DNC network for about a year, but all were expelled over the past weekend in a major computer cleanup campaign, the committee officials and experts said.

The DNC said that no financial, donor or personal information appears to have been accessed or taken, suggesting that the breach was traditional espionage, not the work of criminal hackers.

The intrusions are an example of Russia's interest in the U.S. political system and its desire to understand the policies, strengths and weaknesses of a potential future president — much as American spies gather similar information on foreign candidates and leaders.

The depth of the penetration reflects the skill and determination of the United States' top cyber adversary as Russia goes after strategic targets, from the White House and State Department to political campaign organizations.

"It's the job of every foreign intelligence service to collect intelligence against their adversaries," said Shawn Henry, president of CrowdStrike, the cyber firm called in to handle the DNC breach and a former head of the FBI's cyber division. He noted that it is extremely difficult for a civilian organization to protect itself from a skilled and determined state such as Russia.

"We're perceived as an adversary of Russia," he said. "Their job when they wake up every day is to gather intelligence against the policies, practices and strategies of the U.S. government. There are a variety of ways. [Hacking] is one of the more valuable because it gives you a treasure trove of information."

Russian President Vladimir Putin has spoken favorably about Trump, who has called for better relations with Russia and expressed skepticism about NATO. But unlike Clinton, whom the Russians probably have long had in their spy sights, Trump has not been a politician for very long, so foreign agencies are playing catch-up, analysts say.

"The purpose of such intelligence gathering is to understand the target's proclivities," said Robert Deitz, former senior councillor to the CIA director and a former general counsel at the National Security Agency. "Trump's foreign investments, for example, would be relevant to understanding how he

*(*Continued On The Following Page)*

would deal with countries where he has those investments" should he be elected, Deitz said.

"They may provide tips for understanding his style of negotiating. In short, this sort of intelligence could be used by Russia, for example, to indicate where it can get away with foreign adventurism."

Other analysts noted that any dirt dug up in opposition research is likely to be made public anyway. Nonetheless, DNC leadership acted quickly after the intrusion's discovery to contain the damage.

"The security of our system is critical to our operation and to the confidence of the campaigns and state parties we work with," said Rep. Debbie Wasserman Schultz (D-Fla.), the DNC chairwoman. "When we discovered the intrusion, we treated this like the serious incident it is and reached out to CrowdStrike immediately. Our team moved as quickly as possible to kick out the intruders and secure our network."

Clinton called the intrusion "troubling," in an interview with Telemundo. She also said, "So far as we know, my campaign has not been hacked into," and added that cybersecurity is an issue that she "will be absolutely focused on" if she becomes president. '"Because whether it's Russia, or China, Iran or North Korea more and more countries are using hacking to steal our information, to use it to their advantage," she said.

A spokeswoman for the Trump campaign referred questions to the Secret Service.

DNC leaders were tipped to the hack in late April. Chief executive officer Amy Dacey got a call from her operations chief saying that their information technology team had noticed some unusual network activity.

"It's never a call any executive wants to get, but the IT team knew something was awry," Dacey said. And they knew it was serious enough that they wanted experts to investigate.

That evening, she spoke with Michael Sussmann, a DNC lawyer who is a partner with Perkins Coie in Washington. Soon after, Sussmann, a former federal prosecutor who handled computer crime cases, called Henry, whom he has known for many years.

Within 24 hours, CrowdStrike had installed software on the DNC's computers so that it could analyze data that could indicate who had gained access, when and how.

The firm identified two separate hacker groups, both working for the Russian government, that had infiltrated the network, said Dmitri Alperovitch, CrowdStrike co-founder and chief technology officer. The firm had analyzed other breaches by both groups over the last two years.

*(*Continued On The Following Column)*

One group, which CrowdStrike had dubbed Cozy Bear, had gained access last summer and was monitoring the DNC's email and chat communications, Alperovitch said.

The other, which the firm had named Fancy Bear, broke into the network in late April and targeted the opposition research files. It was this breach that set off the alarm. The hackers stole two files, Henry said. And they had access to the computers of the entire research staff — an average of about several dozen on any given day.

The computers contained research going back years on Trump. "It's a huge job" to dig into the dealings of somebody who has never run for office before, Dacey said.

CrowdStrike is not sure how the hackers got in. The firm suspects they may have targeted DNC employees with "spearphishing" emails. These are communications that appear legitimate — often made to look like they came from a colleague or someone trusted — but that contain links or attachments that when clicked on deploy malicious software that enables a hacker to gain access to a computer. "But we don't have hard evidence," Alperovitch said.

The two groups did not appear to be working together, Alperovitch said. Fancy Bear is believed to work for the GRU, or Russia's military intelligence service, he said. CrowdStrike is less sure of whom Cozy Bear works for but thinks it might be the Federal Security Service or FSB, the country's powerful security agency, which was once headed by Putin.

The lack of coordination is not unusual, he said. "There's an amazing adversarial relationship" among the Russian intelligence agencies, Alperovitch said. "We have seen them steal assets from one another, refuse to collaborate. They're all vying for power, to sell Putin on how good they are."

The two crews have "superb operational tradecraft," he said. They often use previously unknown software bugs — known as "zero-day" vulnerabilities — to compromise applications. In the DNC's case, the hackers constantly switched tactics to maintain a stealthy presence inside the network and used built-in Windows tools so that they didn't have to resort to malicious code that might trigger alerts. "They flew under the radar," Alperovitch said.

(*Continued On The Following Page)

The two groups have hacked government agencies, tech companies, defense contractors, energy and manufacturing firms, and universities in the United States, Canada and Europe as well as in Asia, he said.

Cozy Bear, for instance, compromised the unclassified email systems of the White House, State Department and Joint Chiefs of Staff in 2014, Alperovitch said.

"This is a sophisticated foreign intelligence service with a lot of time, a lot of resources, and is interested in targeting the U.S. political system," Henry said. He said the DNC was not engaged in a fair fight. "You've got ordinary citizens who are doing hand-to-hand combat with trained military officers," he said. "And that's an untenable situation."

Russia has always been a formidable foe in cyberspace, but in the last two years "there's been a thousand-fold increase in its espionage campaign against the West," said Alperovitch, who is also a senior fellow at the Atlantic Council. "They feel under siege."

Western sanctions, imposed after Russia's annexation of Crimea in Ukraine, have hurt the economy and led the government to increase its theft of intellectual property to limit the impact of import restrictions, he said.

And Russia's growing isolation has increased the need for intelligence to understand and influence political decisions in other countries, he added.

CrowdStrike is continuing the forensic investigation, DNC lawyer Sussmann said. "But at this time, it appears that no financial information or sensitive employee, donor or voter information was accessed by the Russian attackers," he said.

The firm has installed special software on every computer and server in the network to detect any efforts by the Russian cyber spies to break in again. "When they get kicked out of the system," Henry predicted, "they're going to try to come back in."

Bombardier CS100 Aircraft Awarded Type Validation

As the newest single-aisle aircraft to enter service in close to 30 years, the C Series is readying to deliver to launch operator SWISS at the end of June 2016

Bombardier Commercial Aircraft announced today that its CS100 aircraft has been awarded Type Validation by the European Aviation Safety Agency (EASA) and the Federal Aviation Administration (FAA) following a comprehensive testing program. The EASA and FAA validations follow the CS100 aircraft Type Certification awarded by Transport Canada in December 2015.

EASA's validation paves the way for the delivery of the first CS100 aircraft to launch operator Swiss International Air Lines ("SWISS") at the end of June and the aircraft's entry-into-service in July 2016. The FAA validation is a required precursor to operation of the aircraft in the U.S.

"In the same week that our C Series aircraft surpassed 5,000 flight hours and the first SWISS aircraft readies for its first flight, we are celebrating another very proud moment with the receipt of the CS100 aircraft EASA and FAA Type Validations. I congratulate our teams for all their hard work in delivering these latest significant accomplishments," said Robert Dewar, Vice President, C Series Program, Bombardier Commercial Aircraft. "As we move quickly towards the delivery of the first CS100 aircraft to SWISS, we are gratified that several aviation leaders are confirming what we have been saying all along -- the C Series aircraft will open up new opportunities for operators, while delivering unrivalled economic advantages, performance, and environmental credentials."

"Obtaining the CS100 aircraft Type Validations from EASA and the FAA marks one of the final chapters in our very successful test program," said François Caza, Vice President, Product Development and Chief Engineer and Head of Bombardier's Design Approval Organization. "Achieving these latest milestones is a direct result of the quality of the work by our highly skilled employees who were involved in the program as well as from the solid collaboration we established with our suppliers.

The Government of Iraq - AC-208 Sustainment, Logistics, and Spares Support

The State Department has made a determination approving a possible Foreign Military Sale to the Government of Iraq for AC-208 sustainment, logistics, and spares support. The estimated cost is $181 million. The Defense Security Cooperation Agency delivered the required certification notifying Congress of this possible sale today.

The Government of Iraq has requested a possible sale of a five-year sustainment package for its AC/RC-208 fleet that includes: operational, intermediate, and depot-level maintenance; spare parts; component repair; publication updates; maintenance training; and logistics. Also included in this sale are Contract Logistics Services (CLS), training services, and Contract Engineering Services. There is no MDE associated with this possible sale. The total overall estimated value is $181 million.

The purchase of this sustainment package will allow the Iraqi Air Force (IqAF) to continue to operate its fleet of eight C-208 light attack and Intelligence, Surveillance, and Reconnaissance (ISR) aircraft beyond the June 2016 end of its existing CLS contract. Limited IqAF maintenance capability necessitates continued CLS. Ultimately, the goal is for the IqAF to become self-sufficient in the areas of aircraft maintenance and logistics training. Iraq will have no difficulty absorbing this support.

The proposed sale will contribute to the foreign policy and national security goals of the United States by helping to improve a critical capability of the Iraq Security Forces in defeating the Islamic State of Iraq and the Levant.

The proposed sale of this equipment and support will not alter the basic military balance in the region.

The principal contractors will be Orbital ATK in Falls Church, Virginia, and Flight Safety International in Flushing, New York. There are no known offset agreements proposed in connection with this potential sale .Implementation of this proposed sale will not require the assignment of any additional U.S. Government or contractor representatives to Iraq. There will be no adverse impact on U.S. defense readiness as a result of this proposed sale. All defense articles and services listed in this transmittal have been authorized for release and export to the Government of Iraq. This notice of a potential sale is required by law and does not mean the sale has been concluded.

Carrier says it will acquire planes through lease purchase Contract is Boeing's first since lifting of sanctions on Iran

Iran Air, the Islamic Republic's state carrier, has signed a memorandum of understanding with Boeing Co. to buy narrow- and wide-body aircraft, in the first transaction by the U.S. planemaker since sanctions were lifted in January.

The purchase includes a mix of 737 and 777 models, Iran Air said in a statement on its website. The carrier will obtain the planes through a lease-purchase agreement, pending clearance from the U.S. and Iran. Boeing said any contracts with Iran's airlines will depend on U.S. government approval.

The country intends to buy 100 jetliners from Boeing, Ali Abedzadeh, director of Iran's Civil Aviation Organization, said in a newspaper interview earlier this week. There were no details on the total figure in Tuesday's statements.

The agreement follows a $27 billion order by Europe's Airbus Group SE in January. The plane manufacturers are competing in one of the few remaining untapped jet markets as a weak global economy saps demand in other regions. Iran says it needs 400 long-range and 100 short-range jets and sees $50 billion in aircraft investments after years of sanctions left its aging fleet in dire need of upgrading.

'Hundreds of Airplanes'

Boeing sees an "opportunity for hundreds of airplanes" in Iran, Randy Tinseth, the planemaker's vice president for marketing, said Tuesday. "Their biggest challenge moving forward is a question of infrastructure, but clearly there's an opportunity."

Iran Air, the country's biggest carrier, currently serves 27 domestic and 29 international routes with an aging fleet that includes Boeing 747s and Fokker NV 100s. It needs the upgraded aircraft as it rolls out a 10-year plan aimed at moving from survival mode to expansion. The airline plans to use wide-body jets to reinstate long-haul routes to such cities as Tokyo and Seoul, which were halted under sanctions.

Plane deals with Iran aren't without risks. The companies must address sanctions that prohibit banks from dollar-based transactions with Iran. Boeing must additionally take into account a political backlash in the U.S., given Iranian leaders' penchant for anti-American rhetoric.

Modine Manufacturing Company (NYSE:MOD) Short Interest Increased By 9.52%

The stock of Modine Manufacturing Company (NYSE:MOD) registered an increase of 9.52% in short interest. MOD's total short interest was 935,200 shares in June as published by FINRA. Its up 9.52% from 853,900 shares, reported previously. With 256,400 shares average volume, it will take short sellers 4 days to cover their MOD's short positions. The short interest to Modine Manufacturing Company's float is 2.18%. The stock increased 1.97% or $0.19 on June 17, hitting $9.83. About 270,989 shares traded hands or 37.49% up from the average. Modine Manufacturing Co. (NYSE:MOD) has risen 10.95% since November 11, 2015 and is uptrending. It has outperformed by 11.13% the S&P500.

Modine Manufacturing Company is a developer, maker and marketer of heat exchangers and systems for use in on-highway and off-highway original equipment maker vehicular applications and to a range of building, industrial and refrigeration markets. The company has a market cap of $475.39 million. The Firm specializes in thermal management systems and components. It currently has negative earnings.

According to TipRanks who tracks the performance of analysts and other financial experts, the analyst consensus on Modine is **Moderate Buy** and the average price target is $12.00, representing a **%0.22** upside. The data is based on 1 analysts that rated Modine in the last 3 months.**See the consensus rating of analysts covering the MOD stock.**

The institutional sentiment increased to 1.07 in Q1 2016. Its up 0.03, from 1.04 in 2015Q4. The ratio is positive, as 15 funds sold all Modine Manufacturing Co. shares owned while 39 reduced positions. 15 funds bought stakes while 43 increased positions. They now own 38.73 million shares or 1.58% less from 39.35 million shares in 2015Q4.

Icm Asset Management Inc Wa holds 1.68% of its portfolio in Modine Manufacturing Co. for 97,705 shares. Oarsman Capital Inc. owns 137,625 shares or 0.81% of their US portfolio. Moreover, Granahan Investment Management Inc Ma has 0.5% invested in the company for 1.24 million shares.

(*Continued On The Following Column)

"Ever job is a self-portrait of the person who does it. Autograph your work with excellence."

The Massachusetts-based Frontier Capital Management Co Llc has invested 0.39% in the stock. Rutabaga Capital Management Llc Ma, a Massachusetts-based fund reported 197,148 shares.

Out of 2 analysts covering Modine Manufacturing (NYSE:MOD), 0 rate it a "Buy", 0 "Sell", while 0 "Hold". This means NaN are positive. Modine Manufacturing has been the topic of 3 analyst reports since August 4, 2015 according to StockzIntelligence Inc.

Addition of Certain Persons and Removal of Certain Persons from the Entity List

This final rule amends the Export Administration Regulations (EAR) by adding twenty-eight persons under thirty-one entries to the Entity List. The twenty-eight persons who are added to the Entity List have been determined by the U.S. Government to be acting contrary to the national security or foreign policy interests of the United States. These twenty-eight persons will be listed on the Entity List under the destinations of Afghanistan, Austria, China, Hong Kong, Iran, Israel, Panama, Taiwan, and the United Arab Emirates (U.A.E.). This final rule also removes three entities from the Entity List under the destinations of Finland, Pakistan and Turkey as the result of requests for removal received by BIS pursuant to the section of the EAR used for requesting removal or modification of an Entity List entity and the End-User Review Committee's (ERC) review of the information provided in the removal requests.