EIB World Trade Headlines

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

April 15, 2017 - Volume 9, Issue 8

TD BANK FINED for OFAC VIOLATIONS

In January of this year, TD Bank was required to pay a civil penalty of $516,105, earning just under a 50 percent discount from the base penalty, for conducting 167 transactions in violation of the Cuba and Iran sanctions programs. TD Bank voluntarily disclosed the violations to OFAC.

TD Bank, which is based in Montreal, Canada, issued a series of letters of credit to Canadian customers engaged in transactions with Iran and Cuba. The transactions, with the letters of credit, were processed through the United States' financial system, thereby triggering United States jurisdiction. A Cuban company owned one Canadian customer, and TD Bank had knowledge of this relationship.

TD Bank also assisted a customer shipping company that transported oil and gas equipment to customers in the Middle East, and was listed as an agent of Specially Designated National located in Iran.

TD Bank also had 62 customers who were Cuban nationals residing in Canada.

TD Bank supervisory personnel knew or should have known of the continuing conduct with the exception of certain violations. OFAC cited TD Bank's weak OFAC compliance program as contributing to the series of violations. On the mitigating side of equation, OFAC cited the fact that TD Bank could have obtained a license to provide services to the Cuban nationals under a general license issued in 2011.

The focus of OFAC's enforcement action centered on TDWIS, TD Bank's securities trading subsidiary. Between 2007 and 2013, TDWIS, the subsidiary company opened trading accounts for 4 individuals subject to the Iran and Cuba sanctions, and processed almost four thousand transactions over the six-year period for these four customers. TDWIS processed securities trading transactions for Internaax, an international brokerage firm.

Internaax shared customer and trading information with TDWIS, which in turn processed the transactions through a United States broker-dealer. Both Internaax and TDWIS had sufficient identifying information to recognizer that the proposed transactions were barred under the Cuba and Iran sanctions programs.

NEWSLETTER NOTES

Trump's tone on NAFTA shifts in letter

By Max Ehrenfreund and Damian Paletta, The Washington Post

WASHINGTON – The Trump administration will seek modest – but numerous – changes to the North American Free Trade Agreement, according to a draft of a letter sent to Congress last week, displaying a much more conventional approach to trade negotiation than the dramatic changes President Donald Trump had suggested he planned to seek.

The draft letter suggests a much more diplomatic tone than Trump has threatened to use during NAFTA renegotiations. It says, among other things, that the White House would look to strengthen cooperation under the World Trade Organization, an international group that the Trump administration had suggested in the past it might not abide by.

The draft letter also indicates that Canada and Mexico are the United States' two largest export markets and that the countries have "shared borders" and "shared goals, shared histories and cultures, and shared challenges."

"Compared to some of the campaign rhetoric, the letter seemed quite reasonable and measured," said John Veroneau, a former deputy U.S. trade representative under President George W. Bush. "It didn't strike me as suggesting a departure from the status quo in any significant way."

One section of the letter that is likely to prove controversial appears to call for restricting federal procurement to U.S. suppliers. If the two other countries adopted similar rules in response, U.S. firms that have contracts with Mexico City and Ottawa could lose business, warned Jeff Schott, an expert on trade at the Peterson Institute for International Economics.

NAFTA is a free-trade agreement that went into force in 1994 after the Clinton administration reached a deal with Canada and Mexico. NAFTA has significantly expanded trade between the three countries, but Democrats and Republicans have said the agreement should be changed because they fear it has hurt U.S. workers. Trump has complained that the deal has allowed Mexico to take advantage of the United States, causing an imbalance in the kinds of goods that are shipped across the border and luring away U.S. jobs.

To renegotiate NAFTA, the White House must send a letter to Congress stating its intent. The White House's Office of the U.S. Trade Representative began circulating a letter last week. The White House must formally notify Congress 90 days before it formally begins renegotiating the trade agreement, and when the letter is formally sent to Capitol Hill, that process will start.

*(*Continued On The Following Column)*

"For reasons of scale alone, improving the NAFTA has the greatest potential to benefit the workers, farmers, and firms of the United States," says the draft, which was signed by Stephen Vaughn, the acting U.S. trade representative.

"Basically, in most areas, it's very consistent with the trade negotiating strategies of past administrations," Schott said.

He added, though, that there are several lines in the letter that indicate departures from past policy. One of the objectives listed is to "seek to level the playing field on tax treatment," a brief and cryptic phrase that could suggest duties on Canadian and Mexican products.

During the campaign, Trump floated a tariff of as much as 35 percent on certain goods imported from Mexico. Another possibility is that if Republicans in Congress deliver on their proposal to adjust corporate taxes at the border, the administration's negotiators would want to make sure that Mexico and Canada are ready to accept the change.

Other language in the letter suggests the administration is skeptical of a process for resolving disputes between governments and multinational firms, whose critics argue it impinges on U.S. sovereignty by giving international tribunals authority that would otherwise belong to U.S. courts.

Yet the letter does not explicitly call for ending the process, known as investor-state dispute settlement. "They put a lot of code words in there about that, but there's still some ambiguity," Schott said.

There were only a couple of passages in the letter that seemed to reflect Trump's stated policy of putting the interests of U.S. workers first. One, Veroneau noted, was the section on "rules of origin," which govern how much raw material from outside North America can be used in products that are manufactured in Canada, Mexico or the United States and sold under NAFTA's favorable terms.

The letter also calls for stronger intellectual-property rights and a commitment from Mexico and Canada not to impose customs duties on digital products.

The letter is still in draft form and is likely to be changed before it is formally sent and received on Capitol Hill.

"NAFTA is the worst trade deal maybe ever," Trump said in a debate with Democratic presidential nominee Hillary Clinton in September. "It's a defective agreement."

Trump has said that if Mexico does not agree to the United States' demands in the renegotiations, he probably would withdraw from NAFTA. But the letter does not include this threat and suggests that a reworked trade deal is possible.

Trump Is Now Preparing Executive Orders to Review All 14 U.S. Trade Deals

The Trump administration is preparing new executive order s to re-examine all 14 U.S. free trade agreements and review government procurement policies to aid American companies, two administration officials said.

The North American Free Trade Agreement (NAFTA) with Mexico and Canada will top the list of trade deals to be reviewed, which affect 20 countries from the Americas to Asia, the officials told Reuters. They spoke on condition of anonymity because the orders were still being developed.

They said on Wednesday that the trade deal and procurement review order s were among several executive actions that the Trump administration is preparing on trade. The timing of the orders is unclear, but they could start to be rolled out next week, the officials said.

Politico first reported the plan for the two order s, quoting a senior administration official as saying the trade order s would help shift the White House narrative "to a place where the president can really shine."

The fate of Trump 's first major legislative effort in Congress, a measure to replace the 2010 Obamacare health law, remains uncertain amid stiff opposition from conservative Republicans. The House of Representatives had to delay a vote on the bill on Thursday due to insufficient support for the legislation.

The order s to review existing trade deals and public procurement policies would be largely symbolic, as the administration has already announced its intention to renegotiate NAFTA, with plans to formally notify Congress of its intention to launch talks in the coming weeks.

Early last month, White House spokesman Sean Spicer said, "We're going to re-examine all the current trade deals, figure out if we can improve them."

The U.S. bilateral and multilateral trade deals cover these countries: Australia, Bahrain, Canada, Chile, Colombia, Costa Rica, the Dominican Republic, El Salvador, Guatemala, Honduras, Israel, Jordan, Mexico, Morocco, Nicaragua, Oman, Panama, Peru, Singapore and South Korea.

Media representatives for the White House and the U.S. Trade Representatives' office declined to comment on any forthcoming executive orders.

*(*Continued On The Following Column)*

Senator Orrin Hatch, the Utah Republican who chairs the Senate Finance Committee, said he would welcome order s to review trade deals if that means it accelerated negotiations on changing them.

"I think we've got to start moving," Hatch told reporters on Wednesday. "If he wants to do these unilaterally or bilaterally, he's got to get going on them."

Trump 's trade officials, including White House adviser Peter Navarro, and Commerce Secretary Wilbur Ross, have long said that NAFTA's rules-of-origin provisions need to be tightened to exclude more components from outside the trading bloc. NAFTA requires cars and trucks to have only 62.5% North American content, providing significant opportunities for Asian manufacturers to provide parts.

The procurement review would be in line with Trump 's "Buy American, Hire American" campaign push and could win some allies among Democrats in Congress. These include Senators Tammy Baldwin of Wisconsin and Jeff Merkley of Oregon, who urged the White House in a recent letter to exclude U.S. government contracts from NAFTA and restrict waivers that allow more foreign companies to bid on public procurements.

But news of the potential trade order s did not impress Republican Senate Agriculture Committee Chairman Pat Roberts of Kansas.

"I'm more interested in getting our trade representative passed on the Senate floor," Roberts told reporters, referring to Robert Lighthizer, Trump 's choice for U.S. trade representative, whose nomination has been stalled in the Senate.

Roberts also said he wanted to impress upon the White House the importance of trade deals to boost agricultural exports, including a glut of Kansas wheat, amid what he views as a preoccupation with manufactured exports in the administration.

Chinese customs officials have told coal ships to return to North Korea

China ordered ships laden with North Korean coal, the isolated nation's most important export, to return home full this month after promising in February to suspend imports of the fuel for the rest of the year.

On Monday evening, Reuters reported a fleet of cargo ships from the country was returned to the North Korean city of Nampo after Chinese customs officials told trading companies to send coal shipments back. A map that the agency published shows nearly a dozen vessels leaving China in the direction of the port.

China suspended all imports of coal from North Korea on Feb. 26 to abide with a United Nations Security Council resolution meant to punish the country and its authoritarian leader, Kim Jong Un, for testing nuclear weapons and launching ballistic missiles. The resolution, passed in December, prohibits member states from importing more than $400 million of North Korean coal in 2017, an amount set so as to not have "adverse humanitarian consequences for the country's civilian population."

Coal is North Korea's biggest export and China is, by far, the product's biggest buyer. The fossil fuel accounts for 34-40 percent of the country's exports and remains a financial lifeline for the isolated dictatorship, The New York Times reports. Shortly after the suspension was announced, Pyongyang fired back at its most powerful ally.

"This country, styling itself a big power, is dancing to the tune of the US while defending its mean behavior," the North's state-run news agency said.

Chinese officials rejected that notion, saying the country was ending imports because it had nearly reached the level set by UN restrictions.

"According to our statistics, China has already approached the upper limits of coal imports from North Korea," Chinese Foreign Ministry spokesman Geng Shuang said during a news briefing in February. "So because of this, we have stopped imports of coal from North Korea with a responsible attitude."

However, analysts have cast doubt on that sentiment, saying it's unlikely China was able to import enough coal by the end of February to reach the $400 million threshold.

*(*Continued On The Following Column)*

"Unless China has other sources of coal imports from North Korea that were not accounted for in the customs data, China unilaterally adopted punitive measures on North Korea that were not required by the UN Security Council Resolution," wrote Yun Sun, a fellow at the think tank The Stimson Center, on 38 North.

The move may signal China's annoyance with the North's continued weapons development, and rifts have grown in recent months between the two countries, particularly over the assassination of Kim Jong Un's half brother in Malaysia this year.

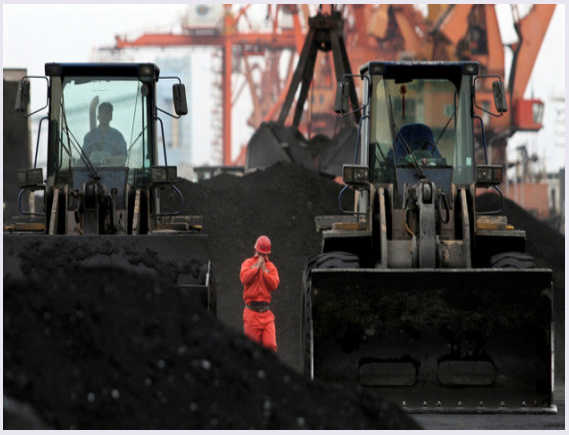
While China's action was met with ire from the North, the country has flouted its own promises before. In 2016, the Chinese government said it would abide by UN sanctions made that March, only to import record amounts of coal from the country the following August, citing "people's well-being."

The country has been unwilling to destabilize its southern neighbor, which provides a vital buffer zone between China and South Korea, a long-time U.S. ally and host to American military bases.

But the North has continued to draw international condemnation over an ongoing string of missile launches. Earlier this month, the country launched a ballistic missile days before President Donald Trump was set to meet China's Xi Jinping. The move sparked a terse rebuke from the U.S.

"The United States has spoken enough about North Korea," Secretary of State Rex Tillerson said. "We have no further comment."

China, still hungry for coal, has rapidly increased imports from the United States after several years of inactivity, Reuters reports.



Trump Gutted The State Department And Half Of Top Jobs Are Still Unfilled

WASHINGTON — Ten weeks after the Trump administration unceremoniously pushed out several top-level State Department officials, their positions remain unfilled, and more than half of the positions listed on the agency's leadership chart are vacant or occupied by temporary acting officials.

Current and former State Department officials are concerned the government's main diplomatic arm is ill-equipped in a time of need. And the persisting vacancies raise questions about the White House's ability or willingness to find capable personnel to fill critical posts.

The staffing issue dates back to January, when, just days into his presidency, Trump notified some of the highest-ranking diplomats at Foggy Bottom that their services were no longer needed. In a move described by officials as an effort to "clean house," Trump pushed out the undersecretary for arms control, the undersecretary for management, the assistant secretary for administration, the assistant secretary for consular affairs and the director of the office for foreign missions. He did not line up replacements for those positions.

Veteran diplomats feared the Trump administration was executing a purge, prioritizing loyalty over know-how. And those fears intensified as several holdovers from previous administrations voluntarily quit their jobs.

Over two months later, the president has yet to find any loyalists to fill those top staffing voids and numerous others. Indeed, it appears that the only person Trump has nominated for a senior position at the State Department is someone with no prior diplomatic experience at all: Secretary of State Rex Tillerson.

The Trump administration has made it abundantly clear that it sees the State Department as less valuable than past administrations have. The president's budget suggested paring back the department's budget by nearly one-third. And his appointment of an oil man with no diplomatic experience as secretary of state suggests he doesn't fully conceive of diplomacy as major geopolitical tool.

But the neglect goes well beyond financial commitments and the man at the top. Tillerson is currently running an agency with no deputy and significantly fewer undersecretaries and assistant secretaries than his predecessors had.

*(*Continued On The Following Column)*

There are also nearly three dozen unoccupied senior positions designed to tackle specific current issues or conflicts. Right now, there is no State Department special envoy assigned to deal with the Six Party Talks aimed at curbing North Korea's nuclear program, the Israeli-Palestinian conflict, Sudan and South Sudan, Myanmar, or Afghanistan and Pakistan. There is also no special envoy tasked with outreach to Muslim communities, combatting anti-Semitism or climate change. The Trump administration is considering doing away entirely with several of these positions, Bloomberg reported in February.

Asked if there were plans to replace the high-level staffers who have left since Trump's inauguration, a State Department spokeswoman said only that the department had no personnel announcements.

"Acting career professionals are currently fulfilling positions as needed," she wrote in an email. "We continue to have a deep bench of experienced career professionals serving in key positions that are highly capable and able to help the Secretary lead the Department."

It's not unusual for new presidents to fill top State Department positions and ambassadorships with individuals of their own choosing. But for the sake of continuity and smooth governance, career officials are usually given advance notice before they're asked to resign. Tom Countryman, the former assistant secretary for international security and nonproliferation, found out he had lost his job while he was traveling to Rome for a meeting on nuclear weapons in January. He cut the trip short, headed back to Washington and cleared out his desk.

Previous administrations have often left career officials in place until their successors are named. That's because the scores of civil servants who remain onboard after the presidential transition rely on the heads of their departments for cues about changes in priorities and policies. Acting officials can be effective short-term managers, but the temporary nature of their tenure can limit their ability and willingness to decisively steer policy.

"'Acting' replacements can hold down the fort for awhile. But other countries pay attention to things like whether you've been selected by the president and confirmed by the senate," Jonathan Finer, former chief of staff and director of policy planning at the State Department, wrote last month. "Over time, vacancies will weaken U.S. diplomacy and force more and more business onto the desk of either the secretary or the White House. One wonders if that may be the point," he continued.

(*Continued On The Following Page)

Trump appears to be in no rush to rebuild the neutered State Department. According to an analysis by Quartz, 57 countries and territories worldwide (including the Vatican) do not currently have a U.S. ambassador. That is partly due to a December order from Trump's transition team for all politically appointed ambassadors to leave their posts by Inauguration Day.

Since then, only two ambassadors have been replaced — U.S. Ambassador to the United Nations Nikki Haley and U.S. Ambassador to Israel David Friedman. The Senate Foreign Relations Committee has received nominations for diplomats to serve in Japan, China, Senegal, and the Republic of Congo, committee spokesman Sean Bartlett told The Huffington Post.

There are no senior State Department nominations pending before the committee, Bartlett said.

The sparse staffing at the State Department is consistent with Trump's call to slash the department's budget and his apparent willingness to dispatch close allies, including his family members, to conduct negotiations abroad in lieu of professional diplomats.

When the president wanted to send a representative to Israel and the Palestinian territories to explore options to broker a peace agreement, he chose his longtime lawyer Jason Greenblatt. (Greenblatt has worked closely with State Department officials.) Trump's son-in-law, Jared Kushner, has already served as one of the president's top advisers on relations with Canada, Mexico, China, Israel and the Palestinian territories. It appears Kushner has also added Iraq and counter-ISIS efforts to his portfolio.

When the staff exodus at the State Department began in January, there were indications that Trump planned to quickly replace at least some of the outgoing officials. The White House was expected to name a deputy to serve under Tillerson "within a few days," The Washington Post reported at the time. Neoconservative State Department veteran Elliott Abrams was reportedly a top candidate for the spot until Trump learned that Abrams had criticized him during the presidential race.

Tillerson still has no deputy.

Why Printers Still Pose a Security Threat

DARKREADING.COM March 8, 2017

Newly discovered security flaws in popular printers remind us how networked devices continue to put users at risk.

Networked printers for years have left gaping holes in home and office network security. Today, experts continue to find flaws in popular laser printers, which are putting businesses at risk.

Experts at the University Alliance Ruhr recently announced vulnerabilities in laser printers from manufacturers including Dell, HP, Lexmark, Samsung, Brother, and Konica. The flaws could permit print docs to be captured, allow buffer overflow exploits, disclose passwords, or cause printer damage.

Up to 60,000 currently deployed printers could be vulnerable, they estimate.
When unprotected, printers expose users to several types of attacks, says Jeremiah Grossman, chief of

security strategy at SentinelOne.

Hackers can use vulnerabilities to capture old printer logs, which may contain sensitive information. They may also use these flaws to establish their foothold in a networked device and move laterally throughout the organization to gather data.

Some attackers want to wreak havoc outside a single business. With networked printers under their control, a cybercriminal may use one company's bandwidth to perform DDoS attacks on other organizations and individuals around the world.

These examples are among the many types of damage that will continue to threaten security as part of the growing Internet of Things, Grossman predicts.

"Most of the time, printers are not going to be terribly different from any IoT device," he explains. Hackers who find vulnerabilities in the web interface can take over, as they could for any device connected to the network.

The difference, of course, is printers have been around far longer than most IoT products. So why is their security still a problem?

Part of the issue is lack of awareness. "Normally, the purchasers of network-connected printers aren't concerned," he says. "'Why should I be concerned about a printer?' they ask. "But it's not just a printer; it's a computer inside a printer and should be treated as such."

*(*Continued On The Following Page)*

Ownership is another factor, says Ed Wingate, vice president and general manager of JetAdvantage Solutions at HP. Printers are shared devices, and it's often unclear whether they belong to IT, facilities, or the team responsible for purchasing them. "This leads to ambiguity over who should control the security of each device," he says.

There is also the longstanding issue of vendors not supporting patches on older devices, a problem that relates to dysfunctionality in the market, says Grossman. Vendors are more relaxed about security because they aren't liable when devices are not secure, he explains.

This presents a market failure that will be difficult to correct because patches won't be made available. Even when they are, devices won't be patched often. Grossman views printer security as less of a technical issue and more of a market problem. Businesses have the information they need to protect themselves, he says, but they won't be secure due to lack of incentive in the system.

Wingate adds that implementing intrusion detection solutions is difficult on printers because most have proprietary operating systems, which used to be tougher to hack. "With the increased scale and professionalization of the hacking industry, now, embedded operating systems are equally interesting targets," he says.

Users with printers running proprietary operating systems can't rely on third parties to develop custom anti-virus solutions, he says. Print manufacturers need to build their own.

HP, he says, partnered with intrusion protection software providers to build JetAdvantage Security Manager, which uses a standards-based approach to protect data across enterprise printer fleets. This makes it easier to manage printer settings and switches.

There used to be an expectation that printers should be managed in the same way PCs are, but the print industry didn't do enough to help users do it, Wingate continues. Part of the challenge is helping businesses figure out how to translate PC security into printer security.

Security managers must be alert as printer flaws continue to make headlines.

Printers will become more popular targets over time, Grossman predicts. Threat actors employ techniques that easily accomplish their goals. Right now the easiest vectors include web hacking and email attacks, but they will move to IoT as computers and operating systems get more secure. Printers are low-hanging fruit, he says, and easier to target.

*(*Continued On The Following Column)*

For businesses working to improve their printer security, he advises regularly checking manufacturer websites to see if patches are available. He also recommends isolating printers on local networks, separate from PCs, and disabling out-of-network communication so even if they're hacked, printers can't interact with adversaries outside the organization.

Wingate suggests adopting the same baseline security practices businesses employ for computers; for example, periodically update passwords so sensitive content isn't left in the open for people to steal. He also recommends intrusion detection, another practice people use for their PCs but don't frequently employ on printers.

FBI Chief Calls for Private Sector to Help Battle Cybercrime

CIO.COM March 9, 2017

As the FBI has been expanding and retooling its approach to cyber investigations, Director James Comey stresses need for CISOs to engage with the bureau.

CHESTNUT HILL, Mass. -- FBI Director James Comey has tough words for private sector firms that won't engage with federal law enforcement authorities on cybersecurity, an area where the bureau has been dramatically expanding its investigation and prosecution efforts.

In a keynote address at a cybersecurity conference at Boston College, Comey lamented that most incidents of intrusion and attacks against U.S. businesses go unreported. But when a victim does report a breach to the FBI, such as the damaging attack against Sony in 2014 that was attributed to North Korea, agents will have a much easier time investigating and helping businesses mitigate the damage if they are already somewhat familiar with the target's systems.

"Sony had taken the time to get to know us," Comey said, describing a rapid response to that incident where agents with a baseline familiarity with Sony's systems could hit the ground running.

"If you are the chief information security officer [CISO] of a private enterprise, and you don't know someone at every single FBI office where you have a significant facility, you're not doing your job. Know that you're pushing on an open door," Comey said. "We're not looking to know your private information, but we need to know you in a way so we can help you in a difficult circumstance."

*(*Continued On The Following Page)*

Comey described a multi-pronged initiative underway at the FBI to crack down on cybercrimes that involves recruiting and hiring more cyber experts, improving engagement with outside partners -- including the private sector -- and rethinking the bureau's traditional approach to working cases. The bureaus is also working to bolster deterrence both through hardening systems that might be targeted and winning convictions in more criminal cases.

speculation that he might step down amid tensions with the White House.

He did not address his reported request for the Justice Department to issue a statement refuting President Trump's assertion that his campaign had been wiretapped by former President Obama, nor the unfolding probe into Russian hacking of political targets during the election. Comey participated in a brief question- and-answer session with audience members following his keynote address, but did not take questions from reporters.

A spectrum of threats, an 'evil layer cake'

He did offer that nation-states comprise the most dangerous enemies in the "stack" of cyber adversaries, followed by multi-national hacking syndicates, insider threats, hacktivists and terrorists, the least menacing element of what Comey calls "an evil layer cake."

"The reason I put them at the bottom of the stack is that terrorists are adept at using the internet to communicate, to recruit, to proselytize, but they have not yet turned to using the internet as a tool of destruction in the way that logic tells us certainly will come in the future," Comey said.

Regardless of what type of actor initiates the attack, the FBI is looking at cyber events in a fundamentally different way than conventional crimes that have a clear physical location. If a pedophile is under investigation for crimes in San Francisco, say, the San Francisco field office of the FBI would handle the case. Not so with cyber. Comey said that the bureau is assigning those cases, where the perpetrators could be up the street or halfway around the world, to the field offices that best demonstrate "the chops" to handle specific cyber investigations. So even if a bank in New York was the victim of a cyberattack, the field office in Little Rock, Ark., potentially could take the lead on the case, with support from other offices that might need to conduct investigative work on the physical premises.

"Whichever field office has demonstrated the best ability on that, we're going to give it to that field office," Comey said. "This has a not-unintended consequence of creating competition within the FBI."

*(*Continued On The Following Column)*

Private sector has edge for hiring top cyber talent, money

In addition to reorienting the bureau's internal approach, Comey said that the FBI is trying to step up its recruiting efforts to bring in the next wave of cyber experts, though he acknowledges that competing with private-sector for top talent is a perennial challenge.

"Here's the challenge we face: we cannot compete with you on dough," Comey said. "The pitch we make to people is come be part of this mission. Come be part of something that is really hard, that is really stressful, that does not pay a lot of money, that does not offer you a lot of sleep. How awesome does that sound? The good news is there's a whole lot of people -- young people -- who want to be part of that kind of mission, who want to be part of doing good for a living."

But the difficulties in winning over converts to the bureau's mission are also tied up in a deeper problem, the same perception of the government as an adversary -- or at least something to be avoided -- that has clouded relations with some in the private sector.

Comey wants to dispel the notion of the FBI as "the man," in the Big Brother sense.

"We have to get better at working with the private sector," he said, decrying firms that are subject to a ransomware attack who opt to pay the ransom and enlist a security consultant to help clean up the mess without alerting law-enforcement authorities.

"That is a terrible place to be," he said. "It is a great thing to hire the excellent private-sector companies that are available to do attribution and remediation, but if the information is not shared with us, we will all be sorry. Because you're kidding yourself if you think I'll just remediate this thing and it will go away, because it will never go away."

Paying ransoms, he argues, only emboldens the criminals, and keeping details of the breach in-house hinders law-enforcement authorities from tracking down the perpetrators.

Plea to tech companies to resist outfitting products with unbreakable, default encryption

Comey put in another plug for tech companies to resist the impulse to outfit their products with unbreakable, default encryption, recalling the highly publicized showdown between the FBI and Apple, while calling for all parties in the debate to resist the urge to resort to "bumper-stickering" the other side and rejecting the suggestion of an inherent tradeoff between privacy and security as a false choice.

"It is short-sighted to conclude that our interests are not aligned in this," he said. "We all value privacy. We all value security. We should never have to sacrifice one for the other."

The Internet of Things (IOT) Vulnerabilities

CYBER CRIME & IT SECURITY

Most Security Pros Expect Increasing Attacks on Industrial Internet of Things

A new Dimensional Research survey looked at the rise of Industrial Internet of Things (IIoT) deployment in organizations, and to what extent it is expected to cause security problems in 2017.

Do you expect to see an increase in security attacks on IIoT in 2017?

IIoT are the connected devices in critical infrastructure segments such as energy, utilities, government, healthcare and finance. The study revealed that:

- Ninety-six percent of those surveyed expect to see an increase in security attacks on IIoT in 2017.
- Fifty-one percent said they do not feel prepared for security attacks that abuse, exploit or maliciously leverage insecure IIoT devices.
- Sixty-four percent said they already recognize the need to protect against IIoT attacks, as they continue to gain popularity among hackers.

"Industry professionals know that the Industrial Internet of Things security is a problem today. More than half of the respondents said they don't feel prepared to detect and stop cyber attacks against IIoT," said David Meltzer, chief technology officer at Tripwire. "There are only two ways this scenario plays out: Either we change our level of preparation or we experience the realization of these risks. The reality is that cyber attacks in the industrial space can have significant consequences in terms of safety and the availability of critical operations."

"As Industrial companies pursue IIoT, it's important to understand the new threats that can impact critical operations. Greater connectivity with operational technology (OT) exposes operational teams to the types of attacks that IT teams are used to seeing, but with even higher stakes," said Robert Westervelt, security research manager at IDC. "The concern for a cyber attack is no longer focused on loss of data, but safety and availability. Consider an energy utility as an example – cyber attacks could disrupt power supply for communities and potentially have impact to life and safety."

(*Continued On The Following Column)

Do you expect the use of IIoT devices will increase risk and vulnerability in your organization?

Deployment of IIoT devices

The study's respondents were also asked how they expect their organizations' deployment of IIoT devices to change, and how it will affect their level of vulnerability. It found that:

- Ninety percent expect IIoT deployment to increase.
- Ninety-four percent expect IIoT to increase risk and vulnerability in their organizations.
- When respondents were broken down by company size, both larger companies (96 percent) and smaller companies (93 percent) expect a significant increase in risk caused by the use of IIoT.

Meltzer continued: "The Industrial Internet of Things ultimately delivers value to organizations, and that's why we're seeing an increase in deployments. Security can't be an industry of 'no' in the face of innovation, and businesses can't be effective without addressing risks. The apparent contradiction of known risks and continued deployment demonstrates that security and operations need to coordinate on these issues. While IIoT may bring new challenges and risks, the fundamentals of security still apply. Organizations don't need to find new security controls, rather they need to figure out how to apply security best practices in new environments."

ARRESTS, TRIALS AND CONVICTIONS

Department of Justice Office of Public Affairs

U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts

FSB Officers Protected, Directed, Facilitated and Paid Criminal Hackers

A grand jury in the Northern District of California has indicted four defendants, including two officers of the Russian Federal Security Service (FSB), for computer hacking, economic espionage and other criminal offenses in connection with a conspiracy, beginning in January 2014, to access Yahoo's network and the contents of webmail accounts. The defendants are Dmitry Aleksandrovich Dokuchaev, 33, a Russian national and resident; Igor Anatolyevich Sushchin, 43, a Russian national and resident; Alexsey Alexseyevich Belan, aka "Magg," 29, a Russian national and resident; and Karim Baratov, aka "Kay," "Karim Taloverov" and "Karim Akehmet Tokbergenov," 22, a Canadian and Kazakh national and a resident of Canada.

(*Continued On The Following Page)

The defendants used unauthorized access to Yahoo's systems to steal information from about at least 500 million Yahoo accounts and then used some of that stolen information to obtain unauthorized access to the contents of accounts at Yahoo, Google and other webmail providers, including accounts of Russian journalists, U.S. and Russian government officials and private-sector employees of financial, transportation and other companies. One of the defendants also exploited his access to Yahoo's network for his personal financial gain, by searching Yahoo user communications for credit card and gift card account numbers, redirecting a subset of Yahoo search engine web traffic so he could make commissions and enabling the theft of the contacts of at least 30 million Yahoo accounts to facilitate a spam campaign.

The charges were announced by Attorney General Jeff Sessions of the U.S. Department of Justice, Director James Comey of the FBI, Acting Assistant Attorney General Mary McCord of the National Security Division, U.S. Attorney Brian Stretch for the Northern District of California and Executive Assistant Director Paul Abbate of the FBI's Criminal, Cyber, Response and Services Branch.

"Cyber crime poses a significant threat to our nation's security and prosperity, and this is one of the largest data breaches in history," said Attorney General Sessions. "But thanks to the tireless efforts of U.S. prosecutors and investigators, as well as our Canadian partners, today we have identified four individuals, including two Russian FSB officers, responsible for unauthorized access to millions of users' accounts. The United States will vigorously investigate and prosecute the people behind such attacks to the fullest extent of the law."

"Today we continue to pierce the veil of anonymity surrounding cyber crimes," said Director Comey. "We are shrinking the world to ensure that cyber criminals think twice before targeting U.S. persons and interests."

" The criminal conduct at issue, carried out and otherwise facilitated by officers from an FSB unit that serves as the FBI's point of contact in Moscow on cybercrime matters, is beyond the pale," said Acting Assistant Attorney General McCord. "Once again, the Department and the FBI have demonstrated that hackers around the world can and will be exposed and held accountable. State actors may be using common criminals to access the data they want, but the indictment shows that our companies do not have to stand alone against this threat. We commend Yahoo and Google for their sustained and invaluable cooperation in the investigation aimed at obtaining justice for, and protecting the privacy of their users."

*(*Continued On The Following Column)*

"This is a highly complicated investigation of a very complex threat. It underscores the value of early, proactive engagement and cooperation between the private sector and the government," said Executive Assistant Director Abbate. "The FBI will continue to work relentlessly with our private sector and international partners to identify those who conduct cyber-attacks against our citizens and our nation, expose them and hold them accountable under the law, no matter where they attempt to hide."

"Silicon Valley's computer infrastructure provides the means by which people around the world communicate with each other in their business and personal lives. The privacy and security of those communications must be governed by the rule of law, not by the whim of criminal hackers and those who employ them. People rightly expect that their communications through Silicon Valley internet providers will remain private, unless lawful authority provides otherwise. We will not tolerate unauthorized and illegal intrusions into the Silicon Valley computer infrastructure upon which both private citizens and the global economy rely," said U.S. Attorney Stretch. "Working closely with Yahoo and Google, Department of Justice lawyers and the FBI were able to identify and expose the hackers responsible for the conduct described today, without unduly intruding into the privacy of the accounts that were stolen. We commend Yahoo and Google for providing exemplary cooperation while zealously protecting their users' privacy."

Summary of Allegations
According to the allegations of the Indictment:
The FSB officer defendants, Dmitry Dokuchaev and Igor Sushchin, protected, directed, facilitated and paid criminal hackers to collect information through computer intrusions in the U.S. and elsewhere. In the present case, they worked with co-defendants Alexsey Belan and Karim Baratov to obtain access to the email accounts of thousands of individuals.

Belan had been publicly indicted in September 2012 and June 2013 and was named one of FBI's Cyber Most Wanted criminals in November 2013. An Interpol Red Notice seeking his immediate detention has been lodged (including with Russia) since July 26, 2013. Belan was arrested in a European country on a request from the U.S. in June 2013, but he was able to escape to Russia before he could be extradited.

Instead of acting on the U.S. government's Red Notice and detaining Belan after his return, Dokuchaev and Sushchin subsequently used him to gain unauthorized access to Yahoo's network. In or around November and December 2014, Belan stole a copy of at least a portion of Yahoo's User Database (UDB), a Yahoo trade secret that contained, among other data, subscriber information including users' names, recovery email accounts, phone numbers and certain information required to manually create, or "mint," account authentication web browser "cookies" for more than 500 million Yahoo accounts.

(*Continued On The Following Page)

Belan also obtained unauthorized access on behalf of the FSB conspirators to Yahoo's Account Management Tool (AMT), which was a proprietary means by which Yahoo made and logged changes to user accounts. Belan, Dokuchaev and Sushchin then used the stolen UDB copy and AMT access to locate Yahoo email accounts of interest and to mint cookies for those accounts, enabling the co-conspirators to access at least 6,500 such accounts without authorization.

Some victim accounts were of predictable interest to the FSB, a foreign intelligence and law enforcement service, such as personal accounts belonging to Russian journalists; Russian and U.S. government officials; employees of a prominent Russian cybersecurity company; and numerous employees of other providers whose networks the conspirators sought to exploit. However, other personal accounts belonged to employees of commercial entities, such as a Russian investment banking firm, a French transportation company, U.S. financial services and private equity firms, a Swiss bitcoin wallet and banking firm and a U.S. airline.

During the conspiracy, the FSB officers facilitated Belan's other criminal activities, by providing him with sensitive FSB law enforcement and intelligence information that would have helped him avoid detection by U.S. and other law enforcement agencies outside Russia, including information regarding FSB investigations of computer hacking and FSB techniques for identifying criminal hackers. Additionally, while working with his FSB conspirators to compromise Yahoo's network and its users, Belan used his access to steal financial information such as gift card and credit card numbers from webmail accounts; to gain access to more than 30 million accounts whose contacts were then stolen to facilitate a spam campaign; and to earn commissions from fraudulently redirecting a subset of Yahoo's search engine traffic.

When Dokuchaev and Sushchin learned that a target of interest had accounts at webmail providers other than Yahoo, including through information obtained as part of the Yahoo intrusion, they tasked their co- conspirator, Baratov, a resident of Canada, with obtaining unauthorized access to more than 80 accounts in exchange for commissions. On March 7, the Department of Justice submitted a provisional arrest warrant to Canadian law enforcement authorities, requesting Baratov's arrest. On March 14, Baratov was arrested in Canada and the matter is now pending with the Canadian authorities.

An indictment is merely an accusation, and a defendant is presumed innocent unless proven guilty in a court of law.The FBI, led by the San Francisco Field Office, conducted the investigation that resulted in the charges announced today. The case is being prosecuted by the U.S. Department of Justice National Security Division's Counterintelligence and Export Control Section and the U.S. Attorney's Office for the Northern District of California, with support from the Justice Department's Office of International Affairs.

(*Continued On The Following Column)

Defendants: At all times relevant to the charges, the Indictment alleges as follows:

- Dmitry Aleksandrovich Dokuchaev, 33, was an officer in the FSB Center for Information Security, aka "Center 18." Dokuchaev was a Russian national and resident.

- Igor Anatolyevich Sushchin, 43, was an FSB officer, a superior to Dokuchaev within the FSB, and a Russian national and resident. Sushchin was embedded as a purported employee and Head of Information Security at a Russian investment bank.

- Alexsey Alexseyevich Belan, aka "Magg," 29, was born in Latvia and is a Russian national and resident. U.S. Federal grand juries have indicted Belan twice before, in 2012 and 2013, for computer fraud and abuse, access device fraud and aggravated identity theft involving three U.S.-based e-commerce companies and the FBI placed Belan on its "Cyber Most Wanted" list. Belan is currently the subject of a pending "Red Notice" requesting that Interpol member nations (including Russia) arrest him pending extradition. Belan was also one of two criminal hackers named by President Barack Obama on Dec. 29, 2016, pursuant to Executive Order 13694, as a Specially Designated National subject to sanctions.

- Karim Baratov, aka "Kay," "Karim Taloverov" and "Karim Akehmet Tokbergenov," 22. He is a Canadian and Kazakh national and a resident of Canada.

Victims:

Yahoo; more than 500 million Yahoo accounts for which account information about was stolen by the defendants; more than 30 million Yahoo accounts for which account contents were accessed without authorization to facilitate a spam campaign; and at least 18 additional users at other webmail providers whose accounts were accessed without authorization.

Time Period:

As alleged in the Indictment, the conspiracy began at least as early as 2014 and, even though the conspirators lost their access to Yahoo's networks in September 2016, they continued to utilize information stolen from the intrusion up to and including at least December 2016.

United States and Thailand Discuss Trade Agenda Under Trade and Investment Framework Agreement

BANGKOK, THAILAND – The United States and Thailand met today under the U.S.-Thailand Trade and Investment Framework Agreement (TIFA) to discuss ways to expand trade and address outstanding issues between them. The United States outlined the Trump administration's trade agenda and the priority it places on enhancing ties with countries in the Asia-Pacific region. This agenda includes bilateral trade initiatives aimed at promoting economic growth, job creation, and competitiveness, as well as addressing unfair trade practices.

The two sides reaffirmed the importance of their longstanding alliance and of working together to address barriers and expand market access between them. The United States and Thailand discussed barriers to U.S. exports to Thailand related to customs, agriculture, intellectual property, labor, financial services, and other issues. The interagency teams included, for the United States, officials from the Office of the U.S. Trade Representative, and the U.S. Departments of State, Agriculture, and Commerce; and for Thailand, officials from the Ministries of Commerce, Health, Agriculture and Cooperatives, Labor, Natural Resources and Environment, Digital Economy and Society, as well as Thai Customs, and the Bank of Thailand.

Assistant U.S. Trade Representative for Southeast Asia and the Pacific Barbara Weisel also met with Commerce Minister Apiradi Tantraporn and Industry Minister Dr. Uttama Savanayana to discuss the U.S.-Thailand bilateral trade agenda.

Background:
The United States and Thailand have strong trade ties, which extends back to the 1833 U.S.-Thailand Treaty of Amity and Economic Relations. Thailand is the United States' 21st largest goods trading partner, with two-way goods trade between them totaling $40 billion in 2016.

Enforce and Protect Act (EAPA)

Preventing Evasion of Antidumping and Countervailing Duty Orders

Title IV, Section 421 of the Trade Facilitation and Trade Enforcement Act of 2015 is commonly referred to as The Enforce and Protect Act of 2015 or EAPA. EAPA establishes formal procedures for submitting and investigating antidumping or countervailing allegations of evasion against U.S. importers. U.S. Customs and Border Protection has responsibility for tracking and reporting allegations of evasion from initial receipt, vetting and enforcement actions, to final disposition of an investigation.https://www.cbp.gov/trade/trade-enforcement/tftea/enforce-and-protect-act-eapa

U.S. Travelers' Top Ten Travel Tips

- Take all the travel documents required for the countries you are visiting, as well as identification for your U.S. reentry. U.S. citizens need passports to reenter the country by air. Go to www.travel.state.gov for destination information.
- Declare everything you bring in from abroad, even if you bought it in a duty free shop.
- Be cautious when buying something from street vendors. The merchandise may be counterfeit and/or unsafe and you may have to surrender it when you return home.
- Items brought abroad for personal use or as gifts are eligible for duty exemptions. If you are bringing them back for resale, they are not eligible for duty exemption.
- Be aware of U.S. prohibited merchandise, such as ivory, tortoiseshell products, and counterfeit items.
- Many foreign-made medications are not approved for United States use and are not permitted in the country. When traveling abroad, bring only the medication you will need. Make sure the medication is in the original container.
- Travels to and from Cuba - Before departing on your trip, check the latest information for the full list of prohibited and restricted items on the U.S. Department of the Treasury Cuba Sanctions website, as well as other related government resources.
- Before bringing food to the United States, please check the list of prohibited items. All live animals, birds and bird products may be restricted, quarantined or require certification.
- CBP officers can inspect you and your belongings without a warrant to enforce U.S. laws.

For more information, read the CBP brochure, "Know Before You Go." Request printed copies or view it online at www.cbp.gov/newsroom/publications/cbp-publication-catalogue.

President Trump No Longer thinks NATO Obsolete

"They made a change and now they do fight terrorism. I said it was obsolete. It's no longer obsolete," Trump said during a joint press conference at the White House with NATO Secretary General Jens Stoltenberg.

Last year, Trump called NATO "obsolete" and faulted members of the alliance for "not paying their fair share." At one point during the campaign, he even said he would "certainly look at" pulling the U.S. out of the organization.

This week, however, Trump actually took steps to expand the historic alliance. His administration announced its support for admitting the country of Montenegro into NATO, two weeks after the Senate approved the move.

During his press conference on Wednesday, Trump spoke glowingly of the alliance's long history, but again called on NATO members to "pay their fair share instead of relying on the United States to make up the difference."

"Many have not been doing that," he said. "We'll be talking about that."

Trump did not, however, offer any bellicose demands or ultimatums as he did on the campaign trail.

NATO is not the only issue Trump sees differently now that he is president. On Wednesday, the Trump administration also reversed itself on the Export/Import Bank, Federal Reserve President Janet Yellen and China's currency manipulation.

On Tuesday, Trump also criticized his predecessor Barack Obama for not intervening in Syria in 2013, even though Trump opposed it at the time.

NORTH KOREA THREATENS NUKES

North Korean state media warned on Tuesday of a nuclear attack on the United States at any sign of American aggression as a U.S. Navy strike group steamed toward the western Pacific.

U.S. President Donald Trump, who has urged China to do more to rein in its impoverished neighbor, said in a Tweet that North Korea was "looking for trouble" and the United States would "solve the problem" with or without China's help.

Tension has escalated sharply on the Korean peninsula, with talk of military action by the United States gaining traction following its strikes last week against Syria and amid concerns the reclusive North may soon conduct a sixth nuclear test. North Korea's official Rodong Sinmun newspaper said the country was prepared to respond to any aggression by the United States.

"Our revolutionary strong army is keenly watching every move by enemy elements with our nuclear sight focused on the U.S. invasionary bases not only in South Korea and the Pacific operation theater but also in the U.S. mainland," it said. South Korea's acting President Hwang Kyo-ahn warned of "greater provocations" by North Korea and ordered the military to intensify monitoring and to ensure close communication with the United States.

"It is possible the North may wage greater provocations such as a nuclear test timed with various anniversaries including the Supreme People's Assembly," said Hwang, acting leader since former president Park Geun-hye was removed amid a graft scandal.

Trump said in a Tweet that a trade deal between China and the United States would be "far better for them if they solved the North Korea problem".

"If China decides to help, that would be great," he said. "If not, we will solve the problem without them!"

Trump and his Chinese counterpart Xi Jinping met in Florida last week and Trump pressed Xi to do more to rein in North Korea.

The North convened a Supreme People's Assembly session on Tuesday, one of its twice-yearly sessions attended by leader Kim Jong Un, and reported a successful national budget execution and personnel appointments, official KCNA news agency said.

*(*Continued On The Following Page)*

There was no mention of its nuclear weapons program or being under threat from the United States, according to KCNA.

South Korean officials took pains to quell talk in social media of an impending security crisis or outbreak of war.

“We’d like to ask for precaution so as not to get blinded by exaggerated assessment about the security situation on the Korean peninsula,” Defense Ministry spokesman Moon Sang-kyun said.

Saturday is the 105th anniversary of the birth of Kim Il Sung, the country’s founding father and grandfather of current ruler, Kim Jong Un.

A military parade is expected in the North’s capital Pyongyang to mark the day. North Korea often also marks important anniversaries with tests of its nuclear or missile capabilities in breach of U.N. Security Council resolutions.

Men and women in colorful outfits were singing and dancing on the streets of Pyongyang, illuminated by better lighting than seen in previous years, apparently practising for the parade.

Syrian President Bashar al-Assad sent a message of congratulations to mark the event, lambasting “big powers” for their “expansionist” policy.

“The friendly two countries are celebrating this anniversary and, at the same time, conducting a war against big powers’ wild ambition to subject all countries to their expansionist and dominationist policy and deprive them of their rights to self-determination,” the North’s KCNA news agency quoted the message as saying.

The North’s foreign ministry, in a statement carried by KCNA, said the U.S. Navy strike group’s approach showed Washington’s “reckless moves for invading had reached a serious phase”.

“We never beg for peace but we will take the toughest counteraction against the provocateurs in order to defend ourselves by powerful force of arms and keep to the road chosen by ourselves,” an unidentified ministry spokesman said.

North Korea and the rich, democratic South are technically still at war because their 1950-1953 conflict ended in a truce, not a peace treaty. The North regularly threatens to destroy the South and its main ally, the United States.

RUSSIAN WORRIES

North Korea is emerging as one of the most pressing foreign policy problems facing the Trump administration.

*(*Continued On The Following Column)*

The North has conducted five nuclear tests, two of them last year, and is working to develop nuclear-tipped missiles that can reach the United States.

The Trump administration is reviewing its policy towards North Korea and has said all options are on the table, including military strikes, but U.S. officials said non-military action appeared to be at the top of the list.

Russia’s foreign ministry, in a statement ahead of a visit by U.S. Secretary of State Rex Tillerson, said it was concerned about many aspects of U.S. foreign policy, particularly on North Korea.

“We are really worried about what Washington has in mind for North Korea after it hinted at the possibility of a unilateral military scenario,” the ministry said.

“It’s important to understand how that would tally with collective obligations on de-nuclearising the Korean peninsula, something that is underpinned in U.N. Security Council resolutions.”

Russia condemned U.S. cruise missile strikes on a Syrian air base on Friday, calling them an illegal attack on a sovereign state.

The U.S. Navy strike group Carl Vinson was diverted from port calls to Australia and would move toward the western Pacific Ocean near the Korean peninsula as a show of force, a U.S. official told Reuters over the weekend.

U.S. officials said the strike group would take more than a week to reach waters near the Korean peninsula.

China and South Korea agreed on Monday to impose tougher sanctions on North Korea if it carried out nuclear or long-range missile tests, a senior official in Seoul said.

On Tuesday, a fleet of North Korean cargo ships was heading home, most of the vessels fully laden, after China ordered its trading companies to return the coal to curb the trade, sources with direct knowledge of the trade said.

The order was given on April 7, just as Trump and Xi were set for the summit where they agreed the North Korean nuclear advances had reached a “very serious stage”, Tillerson said.

Following repeated missile tests that drew international criticism, China banned all imports of North Korean coal on Feb. 26, cutting off the country’s most important export product.

The North is seen ready to conduct its sixth nuclear test at any time, with movements detected by satellite at its Punggye-ri nuclear test site.

Russia Veto UN Council Resolution on Syria China abstained.

April 12, 2017
UNITED NATIONS, April 12 (Reuters) - Russia blocked a Western effort at the U.N. Security Council on Wednesday to condemn last week's deadly gas attack in Syria and push Moscow's ally President Bashar al-Assad to cooperate with international inquiries into the incident.

It was the eighth time during Syria's six-year-old civil war that Moscow has used its veto power on the Security Council to shield Assad's government.

In the latest veto, Russia blocked a draft resolution backed by the United States, France and Britain to denounce the attack in the town of Khan Sheikhoun and tell Assad's government to provide access for investigators and information such as flight plans.

The toxic gas attack on April 4 prompted the United States to launch missile strikes on a Syrian air base and widened a rift between the United States and Russia.

Russian President Vladimir Putin said on Wednesday that trust had eroded between the two countries under U.S. President Donald Trump.

U.S. Secretary of State Rex Tillerson echoed that comment after meetings with Russian leaders in Moscow, saying that relations are at a low point with a low level of trust. Tillerson called for Assad to eventually relinquish power.

China, which has vetoed six resolutions on Syria since the civil war began, abstained from Wednesday's U.N. vote, along with Ethiopia and Kazakhstan. Ten countries voted in favor of the text, while Bolivia joined Russia in voting no.

U.S. Ambassador to the United Nations, Nikki Haley, warned Moscow against protecting Assad, who relies on support from Russia and Iran in his conflict with mostly Sunni Muslim rebels.

"To my colleagues from Russia - you are isolating yourselves from the international community every time one of Assad's planes drop another barrel bomb on civilians and every time Assad tries to starve another community to death," Haley said during a Security Council meeting earlier on Wednesday.

Haley added: "Iran is dumping fuel on the flames of this war in Syria so it can expand its own reach."

ATTACK INVESTIGATION

*(*Continued On The Following Column)*

A fact-finding mission from the Organisation for the Prohibition of Chemical Weapons (OPCW) is investigating last week's attack in a rebel-held area of northern Syria.

If it determines that chemical weapons were used, then a joint U.N./OPCW investigation will look at the incident to determine who is to blame. This team has already found Syrian government forces were responsible for three chlorine gas attacks in 2014 and 2015 and that Islamic State militants used mustard gas.

Britain's U.N. Ambassador Matthew Rycroft told the Security Council that samples taken from the site of the April 4 attack had been analyzed by British scientists and tested positive for the nerve gas sarin. He said Assad's government was responsible.

During a heated Security Council exchange before Wednesday's vote, Russia's deputy U.N. envoy Vladimir Safronkov told the 15-member body that Western countries were wrong to blame Assad for the gas attack.

"I'm amazed that this was the conclusion. No one has yet visited the site of the crime. How do you know that?" he said.

Syria's government has denied responsibility for the attack.

Diplomats said that Russia has put forward a rival draft resolution that expresses concern at last week's gas attack and condemns the U.S. strike on Syria. It was unclear if Moscow planned to put the text to a vote.

Syrian U.N. Ambassador Bashar Ja'afari said Syria had sent dozens of letters to the Security Council, some detailing "the smuggling of sarin from Libya through Turkey on a civilian air plane by using a Syrian citizen."

"Two liters of sarin were transported from Libya through Turkey to terrorist groups in Syria," he said, adding that the government does "not have these weapons."

Western powers say the April 4 gas attack was carried out from the air and that Syrian rebels do not have any aircraft.

China Bets on Sensitive U.S. Start-Ups, Worrying the Pentagon

NYTIMES.COM March 22, 2017

HONG KONG — When the United States Air Force wanted help making military robots more perceptive, it turned to a Boston-based artificial intelligence start-up called Neurala. But when Neurala needed money, it got little response from the American military.

*(*Continued On The Following Page)*

So Neurala turned to China, landing an undisclosed sum from an investment firm backed by a state-run Chinese company.

Chinese firms have become significant investors in American start-ups working on cutting-edge technologies with potential military applications. The start-ups include companies that make rocket engines for spacecraft, sensors for autonomous navy ships, and printers that make flexible screens that could be used in fighter-plane cockpits. Many of the Chinese firms are owned by state-owned companies or have connections to Chinese leaders.

The deals are ringing alarm bells in Washington. According to a new white paper commissioned by the Department of Defense, Beijing is encouraging Chinese companies with close government ties to invest in American start-ups specializing in critical technologies like artificial intelligence and robots to advance China's military capacity as well as its economy.

The white paper, which was distributed to the senior levels of the Trump administration this week, concludes that United States government controls that are supposed to protect potentially critical technologies are falling short, according to three people knowledgeable about its contents, who spoke on the condition of anonymity.

"What drives a lot of the concern is that China is a military competitor," said James Lewis, a senior fellow at the Center for Strategic and International Studies, who is familiar with the report. "How do you deal with a military competitor playing in your most innovative market?"

The Chinese deals can pose a number of issues. Investors could push start-ups to strike partnerships or make licensing or hiring decisions that could expose intellectual property. They can also get an inside glimpse of how technology is being developed and could have access to a start-up's offices or computers.

Trump administration officials and lawmakers are raising broad questions about China's economic relationship with the United States. While the report was commissioned before President Trump took office, some Republicans have called for tighter regulation of foreign takeovers by giving a broader mandate to the Committee on Foreign Investment in the United States. Known as Cfius, the committee reviews foreign takeovers of American companies, but critics say that its scope does not include smaller deals and that it has other weak spots.

Ashton B. Carter, former secretary of defense under President Barack Obama, had tapped Mike A. Brown, the former chief executive of Symantec, the cybersecurity firm, to lead the inquiry into the Chinese investments, according to two of the people aware of the white paper's contents.

*(*Continued On The Following Column)*

A spokesman for the Department of Defense said it "will not discuss the details or components of draft internal working documents."

The size and breadth of the deals are not clear because start-ups and their backers are not obligated to disclose them. Over all, China has been increasingly active in the American start-up world, investing $9.9 billion in 2015, according to data from the research firm CB Insights, more than four times the level the year before.

Neither the high-tech start-ups nor their Chinese investors have been accused of wrongdoing, and experts said much of the activity could be innocent. Chinese investors have money and are looking for returns, while the Chinese government has pushed investment in ways to clean up China's skies, upgrade its industrial capacity and unclog its snarled highways. Proponents of the deals said American limits on technology exports would still apply to American start-ups with Chinese backers.

But the fund flows fit China's pattern of using state-guided investment to help its industrial policy and enhance its technology holdings, as it has recently done with semiconductors. China has also carried out efforts to steal military-related technology.

Still, some start-ups — especially those making hardware rather than money-drawing mobile apps like Snapchat — said Chinese money was sometimes the only available funding. But even a company struggling for money can ultimately come up with a big breakthrough.

Chinese investors have a bigger appetite for risk and a willingness to do deals fast, said Neurala's chief executive, Max Versace.

To demonstrate his software's capabilities to the Air Force, Mr. Versace said, Neurala used its software on a ground drone from Best Buy to make it recognize and follow around the service's secretary, then Deborah Lee James, during a meeting.

"We were told by the secretary of the Air Force, 'Your tech is awesome, we should put it everywhere,'" he said. "No one followed up."

Neurala finally took a minority investment from a Chinese fund called Haiyin Capital as part of a $1.2 million round, Mr. Versace said. He did not disclose the size of Haiyin Capital's commitment. Haiyin Capital is backed by a state-run Chinese company, Everbright Group, according to a statement from one of its subsidiaries.

(*Continued On The Following Page)

American military officials have "figured out a very good way to give $10 billion to Raytheon," he said. "But to give a start-up $1 million to develop a proof of concept? That's still very, very hard."

Late last year, a research firm called Defense Group Inc. argued in a report prepared for Congress that the Neurala investment could give China access to the company's underlying technologies. It also said the deal could create enough uncertainty that American officials would steer clear of Neurala's technology, effectively wasting any American money that had gone into the firm.

Mr. Versace of Neurala said the company took pains to ensure that the Chinese investor had no access to its source code or other important technological information.

To address concerns that it was not tapping innovations from start-ups, the Pentagon in 2015 set up a group called Defense Innovation Unit Experimental to enable investments into promising new companies. While at first it struggled, in 2016 it helped carry off a barrage of deals. The unit also prepared the white paper.

In May 2015, Haiyin Capital also invested an amount it did not disclose in XCOR Aerospace, a Mojave, Calif., commercial space-travel company that makes spacecraft and engines and has worked with NASA. XCOR did not respond to requests for comment.

Haiyin Capital also invested an undisclosed amount in XCOR Aerospace, a Mojave, Calif., commercial space-travel company that makes spacecraft and engines and has worked with NASA. Credit XCOR Aerospace, via PR Newswire

In an interview in Chinese media, Haiyin Capital's founder, Yuquan Wang, said that part of its goal is to build Chinese industrial capabilities and that it can be hard to get space technology into China because of American export controls.

About the fund's investments, Mr. Wang said, "We strive to get a portion of research and development moved back to China so that we can avoid China being only a low-end manufacturer." Haiyin Capital did not respond to a request for comment.

Quanergy, a company that works on the light-detecting sensors used in driverless cars, raised financing last summer that included funds from the partly state-backed Chinese venture fund GP Capital. A few days later, Quanergy purchased people-tracking software from Raytheon for an undisclosed amount. Alongside a wide array of commercial technology, it makes sensors for military driverless vehicles and a security system billed as "the most complete and intelligent 3-D perimeter fencing and intrusion-detection system."

*(*Continued On The Following Column)*

Quanergy did not respond to requests for comment. Its investors also include foreign automakers and South Korea's Samsung.

Chinese investors have also made a push in another industry, flexible electronics. The technology, which the National Research Council has said is a priority for the American military, can help make electronics lighter and easier to attach to anything from a uniform to an airplane.

In 2016, a Silicon Valley start-up called Kateeva that makes machines that print flexible screens raised $88 million from a group of Chinese investors. Three took board seats, including Redview Capital, a spinoff of a firm run by the former Chinese premier Wen Jiabao's son, Wen Yunsong.

Kateeva's chief executive, Alain Harrus, said that while investors in Silicon Valley had begun looking more at hardware companies, raising big rounds for capital-intensive technology can be tough. Kateeva ultimately raised money where its customers were, in China and South Korea. Mr. Harrus said he believed more should be done in America to figure out the best way to nurture and fund core next- generation technologies.

Ken Wilcox, chairman emeritus of Silicon Valley Bank, said in the past six months he had been approached by three different Chinese state-owned enterprises about being their agent in Northern California to buy technology, though he declined.