EIB World Trade Headlines

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

August 15, 2017 - Volume 9, Issue 16

Texas Man Pleads Guilty to Conspiring to Illegally Export Radiation Hardened Integrated Circuits to Russia and China

Peter Zuccarelli, 62, of Plano, Texas pleaded guilty today to conspiring to smuggle and illegally export from the U.S., radiation hardened integrated circuits (RHICs) for use in the space programs of China and Russia, in violation of the International Emergency Economic Powers Act (IEEPA).

Acting Assistant Attorney General for National Security Dana J. Boente and Acting U.S. Attorney Brit Featherston for the Eastern District of Texas made the announcement. The plea was entered before U.S. Magistrate Judge Kimberly Priest-Johnson.

Zuccarelli pleaded guilty to engaging in a conspiracy to smuggle and illegally export from the U.S. items subject to IEEPA, without obtaining licenses from the Department of Commerce. According to the allegations contained in the Information filed against Zuccarelli and statements made in court filings and proceedings, including today's guilty plea:

*(*Continued On The Following Page)*

NEWSLETTER NOTES

Between approximately June 2015 and March 2016, Zuccarelli and his co-conspirators agreed to illegally export RHICs to China and Russia. RHICs have military and space applications, and their export is strictly controlled.

In furtherance of the conspiracy, Zuccarelli's co-conspirator received purchase orders from customers seeking to purchase RHICs for use in China's and Russia's space programs. Zuccarelli received these orders from his co-conspirator, as well as payment of approximately $1.5 million to purchase the RHICs for the Chinese and Russian customers. Zuccarelli placed orders with U.S. suppliers, and used the money received from his co-conspirator to pay the U.S. suppliers. In communications with the U.S. suppliers, Zuccarelli certified that his company, American Coating Technologies was the end user of the RHICs, knowing that this was false. Zuccarelli received the RHICs he ordered from U.S. suppliers, removed them from their original packaging, repackaged them, falsely declared them as "touch screen parts," and shipped them out of the U.S. without the required licenses. He also attempted to export what he believed to be RHICs. In an attempt to hide the conspiracy from the U.S. government, he created false paperwork and made false statements.

At sentencing, Zuccarelli faces a maximum statutory term of five years imprisonment and a maximum fine of $250,000. The maximum statutory sentence is prescribed by Congress and is provided here for informational purposes. If convicted of any offense, the defendant's sentence will be determined by the court after considering the advisory Sentencing Guidelines and other statutory factors. A sentencing hearing will be scheduled after the completion of a presentence investigation by the U.S. Probation Office.

This case is being investigated by the Dallas and Denver Offices of the Department of Homeland Security, Homeland Security Investigations; the FBI; the Department of Commerce, Bureau of Industry and Security, Office of Export Enforcement; and the Department of Defense, Defense Criminal Investigative Service. This case is being prosecuted by the U.S. Attorney's Office for the Eastern District of Texas together with the Counterintelligence and Export Control Section of the Justice Department's National Security Division.

Web Notice

DTAS System outage (08.14.17)
The DTAS information systems will be unavailable from August 16th, 2017 at 4:00AM through 5:00AM for scheduled routine maintenance. The DTAS systems will be available August 16th, 2017 after 5:00AM.

*(*Continued On The Following Column)*

Web Notice: Montenegro's accession to the North Atlantic Treaty (07.31.17)

Pursuant to Montenegro's accession to the North Atlantic Treaty on June 5, 2017, it is the policy of the Department of State that the term "North Atlantic Treaty Organization" ("NATO") in the International Traffic in Arms Regulations ("ITAR") includes Montenegro for the purpose of any subject transactions. The Directorate of Defense Trade Controls ("DDTC") will soon publish a rule in the Federal Register to amend the definition of NATO in ITAR §120.31 accordingly.

Web Notice: Rescission of statutory debarment and reinstatement of Pratt & Whitney Canada Corporation (08.2.17)

On August 2, 2017, DDTC published a Federal Register notice of the rescission of the statutory debarment of Pratt & Whitney Canada Corporation (P&W Canada). The debarment was imposed on the company June 28, 2012. In addition, the notice provides for the reinstatement of eligibility of P&W Canada in accordance with ITAR section 127.11(b). Accordingly, P&W Canada Corporation may participate directly or indirectly in any activities that are subject to the ITAR. The guidance provided by DDTC on July 2, 2012 regarding transactions with P&W Canada entitled "Guidance regarding licensing with United Technologies Corporation subsidiaries. (07.02.12)" is no longer effective.

The Bureau of Industry and Security Presents Update 2017 Conference on Export Controls and Policy Proposed dates: October 3 - 5

The Bureau of Industry and Security (BIS) is preparing for the 30th annual Update Conference on Export Controls and Policy in Washington, D.C. This major outreach activity draws business and government representatives from around the world to learn and exchange ideas about export control issues. It is one of the Department's most notable international trade events.

The proposed dates for Update 2017 will be at the Washington Hilton Hotel. A conference room rate will be available to registered attendees when registration opens. Detailed registration and program information will be available in the coming days.

For additional, information on Update 2017, you may contact the Outreach and Educational Services Division at: UpdateConference@bis.doc.gov or (202) 482-6031.

Bill Browder's Senate Judiciary Committee Hearing Could Explain Anthony Scaramucci's Bizarre Behaviour

HUFF POST, UK
Chris York

On Wednesday 26th July, financier Bill Browder was due to testify before the Senate Judiciary Committee.

In pre-prepared remarks published by The Atlantic, he said: "I hope that my story will help you understand the methods of Russian operatives in Washington and how they use US enablers to achieve major foreign policy goals without disclosing those interests."

On the same day Browder was due to testify, President Trump announced, seemingly out of nowhere, that transgender people will not be allowed to serve in "any capacity" in the US military.

Browder's testimony was then postponed to the next day - the same day The Mooch made headlines when his expletive-ridden tirade was published.

Browder's testimony, which received relatively little coverage, is extraordinary with a senator calling it one of the Senate Judiciary Committee's "most important" hearings.

In it he describes a Russian system of government that operates in the shadows using corruption, blackmail, torture and murder - all led by Vladimir Putin.

Browder said: "Effectively the moment that you enter into their world, you become theirs."

Browder was a very successful businessman operating in Russia and was on friendly terms with Putin but this all changed when he and his lawyer, Sergei Magnitsky, uncovered evidence of a huge $230 million corruption scandal.

*(*Continued On The Following Column)*

The pair reported it to the Russian authorities: "And we waited for the good guys to get the bad guys.

"It turned out that in Putin's Russia, there are no good guys."

Instead of investigating the allegations Browder was himself accused of tax evasion and was barred from reentering Russia after travelling abroad on business.

Magnitsky was jailed and is believed to have been beaten to death in 2009.

Browder said: "Sergei Magnitsky was murdered as my proxy. If Sergei had not been my lawyer, he would still be alive today."

In 2012 the dead lawyer gave his name to the Magnitsky Act which was passed by the US Congress to target Russian human rights abusers by barring them from America and freezing their financial assets.

Browder said of the move: "Putin was furious. Looking for ways to retaliate against American interests, he settled on the most sadistic and evil option of all: banning the adoption of Russian orphans by American families."

But why was Putin so angry at the sanctions? Bowder explains:

For two reasons. First, since 2012 it's emerged that Vladimir Putin was a beneficiary of the stolen $230 million that Sergei Magnitsky exposed.

Recent revelations from the Panama Papers have shown that Putin's closest childhood friend, Sergei Roldugin, a famous cellist, received $2 billion of funds from Russian oligarchs and the Russian state.

It's commonly understood that Mr. Roldugin received this money as an agent of Vladimir Putin. Information from the Panama Papers also links some money from the crime that Sergei Magnitsky discovered and exposed to Sergei Roldugin.

Based on the language of the Magnitsky Act, this would make Putin personally subject to Magnitsky sanctions.

This is particularly worrying for Putin, because he is one of the richest men in the world. I estimate that he has accumulated $200 billion of ill-gotten gains from these types of operations over his 17 years in power.

(*Continued On The Following Page)

He keeps his money in the West and all of his money in the West is potentially exposed to asset freezes and confiscation. Therefore, he has a significant and very personal interest in finding a way to get rid of the Magnitsky sanctions.

The second reason why Putin reacted so badly to the passage of the Magnitsky Act is that it destroys the promise of impunity he's given to all of his corrupt officials.

There are approximately ten thousand officials in Russia working for Putin who are given instructions to kill, torture, kidnap, extort money from people, and seize their property.

Before the Magnitsky Act, Putin could guarantee them impunity and this system of illegal wealth accumulation worked smoothly. However, after the passage of the Magnitsky Act, Putin's guarantee disappeared.

The Magnitsky Act created real consequences outside of Russia and this created a real problem for Putin and his system of kleptocracy.

Interestingly, Donald Trump Jr described his controversial meeting with a Russian lawyer last summer as a "short introductory meeting" focused on the disbanded program that had allowed American adoptions of Russian children.

This Russian lawyer was Natalia Veselnitskaya, a woman Browder describes as part of a "group of Russians acting on behalf of the Russian state".

He adds:

Pyotr Katsyv, father to Denis Katsyv, is a senior Russian government official and well-placed member of the Putin regime; Denis Katsyv was caught by U.S. law enforcement using proceeds from the crime that Sergei Magnitsky uncovered to purchase high-end Manhattan real estate (the case recently settled with the Katsyv's paying $6 million to the U.S. government). Natalia Veselnitskaya was their lawyer.

In addition to working on the Katsyv' s money laundering defense, Ms. Veselnitskaya also headed the aforementioned lobbying campaign to repeal the Magnitsky Act. She hired a number of lobbyists, public relations executives, lawyers, and investigators to assist her in this task.

Her first step was to set up a fake NGO that would ostensibly promote Russian adoptions, although it quickly became clear that the NGO's sole purpose was to repeal the Magnitsky Act.

*(*Continued On The Following Column)*

During the Senate Judiciary Committee, Browder was asked by Senator Lindsey Graham's on the apparent contradiction of Russia allegedly having ties to the unverified dossier on Trump while also rooting for him to win the presidency.

Browder replied: "What you need to understand about the Russians is there is no ideology at all. Vladimir Putin is in the business of trying to create chaos everywhere."

Senator Richard Blumenthal asked: "They've got you both ways: with the carrot of continued bribery, and the stick of exposure and blackmail if you defect?"

Browder replied: "That is how every single one of their relationships work. That's how they grab people and keep them.

"And once you get stuck in with them, you can never leave."

The full transcript of Browder's prepared remarks is as follows...

Chairman Grassley, Ranking Member Feinstein, and members of the committee, thank you for giving me the opportunity to testify today on the Russian government's attempts to repeal the Magnitsky Act in Washington in 2016, and the enablers who conducted this campaign in violation of the Foreign Agents Registration Act, by not disclosing their roles as agents for foreign interests.Before I get into the actions of the agents who conducted the anti-Magnitsky campaign in Washington for the benefit of the Russian state, let me share a bit of background about Sergei Magnitsky and myself.I am the founder and CEO of Hermitage Capital Management. I grew up in Chicago, but for the last 28 years I've lived in Moscow and London, and am now a British citizen. From 1996 to 2005, my firm, Hermitage Capital, was one of the largest investment advisers in Russia with more than $4 billion invested in Russian stocks.Russia has a well-known reputation for corruption; unfortunately, I discovered that it was far worse than many had thought. While working in Moscow I learned that Russian oligarchs stole from shareholders, which included the fund I advised. Consequently, I had an interest in fighting this endemic corruption, so my firm started doing detailed research on exactly how the oligarchs stole the vast amounts of money that they did. When we were finished with our research we would share it with the domestic and international media.

For a time, this naming and shaming campaign worked remarkably well and led to less corruption and increased share prices in the companies we invested in. Why? Because President Vladimir Putin and I shared the same set of enemies. When Putin was first elected in 2000, he found that the oligarchs had misappropriated much of the president's power as well.

(*Continued On The Following Page)

They stole power from him while stealing money from my investors. In Russia, your enemy's enemy is your friend, and even though I've never met Putin, he would often step into my battles with the oligarchs and crack down on them.

That all changed in July 2003, when Putin arrested Russia's biggest oligarch and richest man, Mikhail Khodorkovsky. Putin grabbed Khodorkovsky off his private jet, took him back to Moscow, put him on trial, and allowed television cameras to film Khodorkovsky sitting in a cage right in the middle of the courtroom. That image was extremely powerful, because none of the other oligarchs wanted to be in the same position. After Khodorkovsky's conviction, the other oligarchs went to Putin and asked him what they needed to do to avoid sitting in the same cage as Khodorkovsky. From what followed, it appeared that Putin's answer was, "Fifty percent." He wasn't saying 50 percent for the Russian government or the presidential administration of Russia, but 50 percent for Vladimir Putin personally. From that moment on, Putin became the biggest oligarch in Russia and the richest man in the world, and my anti-corruption activities would no longer be tolerated.

The results of this change came very quickly. On November 13, 2005, as I was flying into Moscow from a weekend away, I was stopped at Sheremetyevo airport, detained for 15 hours, deported, and declared a threat to national security.

Eighteen months after my expulsion a pair of simultaneous raids took place in Moscow. Over 25 Interior Ministry officials barged into my Moscow office and the office of the American law firm that represented me. The officials seized all the corporate documents connected to the investment holding companies of the funds that I advised. I didn't know the purpose of these raids so I hired the smartest Russian lawyer I knew, a 35-year-old named Sergei Magnitsky. I asked Sergei to investigate the purpose of the raids and try to stop whatever illegal plans these officials had.Sergei went out and investigated. He came back with the most astounding conclusion of corporate identity theft: The documents seized by the Interior Ministry were used to fraudulently re-register our Russian investment holding companies to a man named Viktor Markelov, a known criminal convicted of manslaughter. After more digging, Sergei discovered that the stolen companies were used by the perpetrators to misappropriate $230 million of taxes that our companies had paid to the Russian government in the previous year.I had always thought Putin was a nationalist. It seemed inconceivable that he would approve of his officials stealing $230 million from the Russian state. Sergei and I were sure that this was a rogue operation and if we just brought it to the attention of the Russian authorities, the "good guys" would get the "bad guys" and that would be the end of the story.

*(*Continued On The Following Column)*

We filed criminal complaints with every law enforcement agency in Russia, and Sergei gave sworn testimony to the Russian State Investigative Committee (Russia's FBI) about the involvement of officials in this crime.

However, instead of arresting the people who committed the crime, Sergei was arrested. Who took him? The same officials he had testified against. On November 24, 2008, they came to his home, handcuffed him in front of his family, and threw him into pre-trial detention.Sergei's captors immediately started putting pressure on him to withdraw his testimony. They put him in cells with 14 inmates and eight beds, leaving the lights on 24 hours a day to impose sleep deprivation. They put him in cells with no heat and no windowpanes, and he nearly froze to death. They put him in cells with no toilet, just a hole in the floor and sewage bubbling up. They moved him from cell to cell in the middle of the night without any warning. During his 358 days in detention he was forcibly moved multiple times.They did all of this because they wanted him to withdraw his testimony against the corrupt Interior Ministry officials, and to sign a false statement that he was the one who stole the $230 million—and that he had done so on my instruction.Sergei refused. In spite of the grave pain they inflicted upon him, he would not perjure himself or bear false witness.After six months of this mistreatment, Sergei's health seriously deteriorated. He developed severe abdominal pains, he lost 40 pounds, and he was diagnosed with pancreatitis and gallstones and prescribed an operation for August 2009. However, the operation never occurred. A week before he was due to have surgery, he was moved to a maximum security prison called Butyrka, which is considered to be one of the harshest prisons in Russia. Most significantly for Sergei, there were no medical facilities there to treat his medical conditions.

At Butyrka, his health completely broke down. He was in agonizing pain. He and his lawyers wrote 20 desperate requests for medical attention, filing them with every branch of the Russian criminal justice system. All of those requests were either ignored or explicitly denied in writing.

After more than three months of untreated pancreatitis and gallstones, Sergei Magnitsky went into critical condition. The Butyrka authorities did not want to have responsibility for him, so they put him in an ambulance and sent him to another prison that had medical facilities. But when he arrived there, instead of putting him in the emergency room, they put him in an isolation cell, chained him to a bed, and eight riot guards came in and beat him with rubber batons. That night he was found dead on the cell floor.Sergei Magnitsky died on November 16, 2009, at the age of 37, leaving a wife and two children.I received the news of his death early the next morning. It was by far the most shocking, heart-breaking, and life-changing news I've ever received.Sergei Magnitsky was murdered as my proxy.

(*Continued On The Following Page)

If Sergei had not been my lawyer, he would still be alive today.That morning I made a vow to Sergei's memory, to his family, and to myself that I would seek justice and create consequences for the people who murdered him. For the last seven and a half years, I've devoted my life to this cause. Even though this case was characterized by injustice all the way through, the circumstances of Sergei's torture and death were so extreme that I was sure some people would be prosecuted. Unlike other deaths in Russian prisons, which are largely undocumented, Sergei had written everything down. In his 358 days in detention, Sergei wrote over 400 complaints detailing his abuse. In those complaints he described who did what to him, as well as where, how, when, and why. He was able to pass his hand-written complaints to his lawyers, who dutifully filed them with the Russian authorities. Although his complaints were either ignored or rejected, copies of them were retained. As a result, we have the most well-documented case of human rights abuse coming out of Russia in the last 35 years.

When I began the campaign for justice with this evidence, I thought that the Russian authorities would have no choice but to prosecute at least some of the officials involved in Sergei Magnitsky's torture and murder. It turns out I could not have been more wrong. Instead of prosecuting, the Russian authorities circled the wagons and exonerated everybody involved. They even went so far as to offer promotions and state honors to those most complicit in Sergei's persecution.

It became obvious that if I was going to get any justice for Sergei Magnitsky, I was going to have to find it outside of Russia.But how does one get justice in the West for a murder that took place in Russia? Criminal justice is based on jurisdiction: One cannot prosecute someone in New York for a murder committed in Moscow. As I thought about it, the murder of Sergei Magnitsky was done to cover up the theft of $230 million from the Russian Treasury. I knew that the people who stole that money wouldn't keep it in Russia. As easily as they stole the money, it could be stolen from them. These people keep their ill-gotten gains in the West, where property rights and rule of law exist. This led to the idea of freezing their assets and banning their visas here in the West. It would not be true justice but it would be much better than the total impunity they enjoyed.In 2010, I traveled to Washington and told Sergei Magnitsky's story to Senators Benjamin Cardin and John McCain. They were both shocked and appalled and proposed a new piece of legislation called The Sergei Magnitsky Rule of Law Accountability Act. This would freeze assets and ban visas for those who killed Sergei as well as other Russians involved in serious human rights abuse.

*(*Continued On The Following Column)*

Despite the White House's desire to reset relations with Russia at the time, this case shined a bright light on the criminality and impunity of the Putin regime and persuaded Congress that something needed to be done. In November 2012 the Magnitsky Act passed the House of Representatives by 364 to 43 votes and later the Senate 92 to 4 votes. On December 14, 2012, President Obama signed the Sergei Magnitsky Act into law.

Putin was furious. Looking for ways to retaliate against American interests, he settled on the most sadistic and evil option of all: banning the adoption of Russian orphans by American families. This was particularly heinous because of the effect it had on the orphans. Russia did not allow the adoption of healthy children, just sick ones. In spite of this, American families came with big hearts and open arms, taking in children with HIV, Down syndrome, Spina Bifida and other serious ailments. They brought them to America, nursed them, cared for them and loved them. Since the Russian orphanage system did not have the resources to look after these children, many of those unlucky enough to remain in Russia would die before their 18th birthday. In practical terms, this meant that Vladimir Putin sentenced his own, most vulnerable and sick Russian orphans to death in order to protect corrupt officials in his regime.Why did Vladimir Putin take such a drastic and malicious step?

For two reasons. First, since 2012 it's emerged that Vladimir Putin was a beneficiary of the stolen $230 million that Sergei Magnitsky exposed. Recent revelations from the Panama Papers have shown that Putin's closest childhood friend, Sergei Roldugin, a famous cellist, received $2 billion of funds from Russian oligarchs and the Russian state. It's commonly understood that Mr. Roldugin received this money as an agent of Vladimir Putin. Information from the Panama Papers also links some money from the crime that Sergei Magnitsky discovered and exposed to Sergei Roldugin. Based on the language of the Magnitsky Act, this would make Putin personally subject to Magnitsky sanctions.

This is particularly worrying for Putin, because he is one of the richest men in the world. I estimate that he has accumulated $200 billion of ill-gotten gains from these types of operations over his 17 years in power. He keeps his money in the West and all of his money in the West is potentially exposed to asset freezes and confiscation. Therefore, he has a significant and very personal interest in finding a way to get rid of the Magnitsky sanctions.The second reason why Putin reacted so badly to the passage of the Magnitsky Act is that it destroys the promise of impunity he's given to all of his corrupt officials.There are approximately ten thousand officials in Russia working for Putin who are given instructions to kill, torture, kidnap, extort money from people, and seize their property.

(*Continued On The Following Page)

Before the Magnitsky Act, Putin could guarantee them impunity and this system of illegal wealth accumulation worked smoothly. However, after the passage of the Magnitsky Act, Putin's guarantee disappeared. The Magnitsky Act created real consequences outside of Russia and this created a real problem for Putin and his system of kleptocracy.

For these reasons, Putin has stated publicly that it was among his top foreign policy priorities to repeal the Magnitsky Act and to prevent it from spreading to other countries. Since its passage in 2012, the Putin regime has gone after everybody who has been advocating for the Magnitsky Act.

One of my main partners in this effort was Boris Nemtsov. Boris testified in front of the U.S. Congress, the European Parliament, the Canadian Parliament, and others to make the point that the Magnitsky Act was a "pro-Russian" piece of legislation because it narrowly targeted corrupt officials and not the Russian people. In 2015, Boris Nemtsov was murdered on the bridge in front of the Kremlin.Boris Nemtsov's protégé, Vladimir Kara-Murza, also traveled to law-making bodies around the world to make a similar case. After Alexander Bastrykin, the head of the Russian Investigative Committee, was added to the Magnitsky List in December of 2016, Vladimir was poisoned. He suffered multiple organ failure, went into a coma and barely survived.The lawyer who represented Sergei Magnitsky's mother, Nikolai Gorokhov, has spent the last six years fighting for justice. This spring, the night before he was due in court to testify about the state cover up of Sergei Magnitsky's murder, he was thrown off the fourth floor of his apartment building. Thankfully he survived and has carried on in the fight for justice.

I've received many death threats from Russia. The most notable one came from Russian Prime Minister Dmitry Medvedev at the World Economic Forum in Davos, Switzerland, in 2013. When asked by a group of journalists about the death of Sergei Magnitsky, Medvedev replied, "It's too bad that Sergei Magnitsky is dead and Bill Browder is still alive and free." I've received numerous other death threats from Russian sources through text messages, emails, and voicemails. U.S. government sources have warned me about a planned Russian rendition against me. These threats were in addition to numerous unsuccessful attempts that the Russian government has made to arrest me using Interpol or other formal legal assistance channels.

The Russian government has also used its resources and assets to try to repeal the Magnitsky Act. One of the most shocking attempts took place in the spring and summer of last year when a group of Russians went on a lobbying campaign in Washington to try to repeal the Magnitsky Act by changing the narrative of what had happened to Sergei. According to them, Sergei wasn't murdered and he wasn't a whistle-blower, and the Magnitsky Act was based on a false set of facts.

*(*Continued On The Following Column)*

They used this story to try to have Sergei's name taken off of the Global Magnitsky Act that passed in December 2016. They were unsuccessful.Who was this group of Russians acting on behalf of the Russian state? Two men named Pyotr and Denis Katsyv, a woman named Natalia Veselnitskaya, and a large group of American lobbyists, all of whom are described below.

Pyotr Katsyv, father to Denis Katsyv, is a senior Russian government official and well-placed member of the Putin regime; Denis Katsyv was caught by U.S. law enforcement using proceeds from the crime that Sergei Magnitsky uncovered to purchase high-end Manhattan real estate (the case recently settled with the Katsyv's paying $6 million to the U.S. government). Natalia Veselnitskaya was their lawyer.

In addition to working on the Katsyv' s money laundering defense, Ms. Veselnitskaya also headed the aforementioned lobbying campaign to repeal the Magnitsky Act. She hired a number of lobbyists, public relations executives, lawyers, and investigators to assist her in this task.Her first step was to set up a fake NGO that would ostensibly promote Russian adoptions, although it quickly became clear that the NGO's sole purpose was to repeal the Magnitsky Act. This NGO was called the Human Rights Accountability Global Initiative Foundation (HRAGI). It was registered as a corporation in Delaware with two employees on February 18, 2016. HRAGI was used to pay Washington lobbyists and other agents for the anti-Magnitsky campaign. (HRAGI now seems to be defunct, with taxes due.)Through HRAGI, Rinat Akhmetshin, a former Soviet intelligence officer naturalised as an American citizen, was hired to lead the Magnitsky repeal effort. Mr. Akhmetshin has been involved in a number of similar campaigns where he's been accused of various unethical and potentially illegal actions like computer hacking.

Veselnitskaya also instructed U.S. law firm Baker Hostetler and their Washington, D.C.-based partner Marc Cymrot to lobby members of Congress to support an amendment taking Sergei Magnitsky's name off the Global Magnitsky Act. Mr. Cymrot was in contact with Paul Behrends, a congressional staffer on the House Foreign Affairs Committee at the time, as part of the anti-Magnitsky lobbying campaign.

Veselnitskaya, through Baker Hostetler, hired Glenn Simpson of the firm Fusion GPS to conduct a smear campaign against me and Sergei Magnitsky in advance of congressional hearings on the Global Magnitsky Act. He contacted a number of major newspapers and other publications to spread false information that Sergei Magnitsky was not murdered, was not a whistle-blower, and was instead a criminal. They also spread false information that my presentations to lawmakers around the world were untrue.

*(*Continued On The Following Page)*

As part of Veselnitskaya's lobbying, a former Wall Street Journal reporter, Chris Cooper of the Potomac Group, was hired to organize the Washington, D.C.-based premiere of a fake documentary about Sergei Magnitsky and myself. This was one the best examples of Putin's propaganda. They hired Howard Schweitzer of Cozzen O'Connor Public Strategies and former Congressman Ronald Dellums to lobby members of Congress on Capitol Hill to repeal the Magnitsky Act and to remove Sergei's name from the Global Magnitsky bill. On June 13, 2016, they funded a major event at the Newseum to show their fake documentary, inviting representatives of Congress and the State Department to attend.While they were conducting these operations in Washington, D.C., at no time did they indicate that they were acting on behalf of Russian government interests, nor did they file disclosures under the Foreign Agent Registration Act .United States law is very explicit that those acting on behalf of foreign governments and their interests must register under FARA so that there is transparency about their interests and their motives.Since none of these people registered, my firm wrote to the Department of Justice in July 2016 and presented the facts. I hope that my story will help you understand the methods of Russian operatives in Washington and how they use U.S. enablers to achieve major foreign policy goals without disclosing those interests. I also hope that this story and others like it may lead to a change in the FARA enforcement regime in the future. Thank you.

Russia's Remarkable Afghan Comeback

In expanding its embassy staff, signing a security agreement with Afghanistan and pledging to bolster the country's housing sector, Russia is trying to reshape its image among Afghans and exploit disillusionment over the results of 16 years of U.S. intervention, suggests Arturo G. Muñoz in Newsweek. Now, "Russia is enjoying a remarkable comeback in the land that once fought so violently to expel it.

"Regardless of the gains that have been made in some areas, masses of unemployed Afghans have lost hope and are emigrating in unprecedented numbers. Afghan soldiers are fighting valiantly, but terrorist attacks are on the rise and the U.S.-backed Afghan government appears incapable of establishing security across the country. The bulk of U.S. and NATO military forces have departed, aggravating Afghan fears of being abandoned again by the West.

ISIS, Climate Change (and U.S.) Trouble the World: Poll

ISIS and climate change are seen as the two biggest threats to national security across the globe, according to the results of a new Pew Research poll. And American power and influence is seen as more troubling than that of China or Russia.

Sixty-two percent of respondents from a total of 38 countries listed ISIS as a major threat to their country, followed by 61% for climate change. Cyber attacks (51%) and the state of the global economy (51%) were the only other threats cited by at least half of respondents.

Meanwhile, 35% of respondents said they saw U.S. power as a major threat, compared with 31% for both Russia and China.

How Maduro Could Shred Venezuela's Constitution

For years, some critics of Venezuelan President Nicolas Maduro have referred to him as a dictator. Now, following **Sunday's vote to replace the opposition-controlled National Assembly with a new Constituent Assembly**, he might officially earn the moniker, **write Michael Shifter and Ben Raderstorf for *Foreign Affairs***.

"In practice, the constituent assembly is akin to a new super-congress, a body capable of reshaping the government as it wishes and delegitimizing the other institutions of the state without replacing them," they write. "Even if it never produces a new constitution, the assembly's existence could thus provide the means to shutter the legislature, fire the attorney general (who has recently emerged as a nuisance to the government), and postpone future elections indefinitely. In other words, the assembly could effectively shred Venezuela's constitution without replacing it.

Iranian Drone Interferes With USS Nimitz Flight Operations

While operating in international airspace in the central Persian Gulf, an F/A-18E Super Hornet with Strike Fighter Squadron 147, assigned to the aircraft carrier USS Nimitz, had an unsafe and unprofessional interaction with an Iranian QOM-1 unmanned aerial vehicle today, U.S. Central Command officials said.

Despite repeated radio calls to stay clear of active fixed-wing flight operations in vicinity of the USS Nimitz, the QOM-1 executed unsafe and unprofessional altitude changes in the close vicinity of an F/A-18E that was in a holding pattern and preparing to land on the aircraft carrier, officials said. The F/A-18E maneuvered to avoid collision with the QOM-1 resulting in a lateral separation between the two aircraft of about 200 feet and a vertical separation of about 100 feet.

Take Down: Hackers Looking to Shut Down Factories for Pay

The malware entered the North Carolina transmission plant's computer network via email last August, just as the criminals wanted, spreading like a virus and threatening to lock up the production line until the company paid a ransom.

AW North Carolina stood to lose $270,000 in revenue, plus wages for idled employees, for every hour the factory wasn't shipping its crucial auto parts to nine Toyota car and truck plants across North America, said John Peterson, the plant's information technology manager.

The company is just one of a growing number being hit by cyber-criminals looking for a payday.
While online thieves have long targeted banks for digital holdups, today's just-in-time manufacturing sector is climbing toward the top of hackers' hit lists.

Production lines that integrate computer-imaging, barcode scanners and measuring tolerances to a hair's width at multiple points are more vulnerable to malevolent outsiders.

"These people who try to hack into your network know you have a set schedule. And they know hours are meaningful to what you're doing," Peterson said in an interview. "There's only a day and a half of inventory in the entire supply chain. And so if we don't make our product in time, that means Toyota doesn't make their product in time, which means they don't have a car to sell on the lot that next day. It's that tight."

He said that creates pressure on manufacturers to make the criminals go away by paying the sums demanded.

"They may not know what that number is, but they know it's not zero. So what is that number? Where do you flinch?"

Last August at the 2,200-worker Durham transmission factory, the computer virus coursed through the plant's network, flooding machines with data and stopping production for about four hours, Peterson said.

Data on some laptops was lost, but the malware was blocked by a firewall when it tried to exit the plant's network and put the hackers' lock on the plant's computer network.

The plant was hit again in April, this time by different crooks using new malware designed to hold data or devices hostage to force a ransom payment, Peterson said. The virus was contained before affecting production, and no ransom was paid to either group, he said.

*(*Continued On The Following Column)*

Manufacturers, government and financial firms are now the top targets globally for illicit intrusions by criminals, foreign espionage agencies and others up to no good, according to a report this spring by NTT Security.

A survey of nearly 3,000 corporate cybersecurity executives in 13 countries last year by Cisco Systems Inc. found about one out of four manufacturing organizations reported cyberattacks that cost them money in the previous 12 months.

Since 2015, U.S. manufacturers considered "critical" to the economy and to normal modern life, like makers of autos and aviation parts, have been the main targets of cyberattacks — outstripping energy, communications and other critical infrastructure, according to Department of Homeland Security incident response data. The numbers may be imprecise because companies in key industries often don't report attacks for fear of diminished public perception.

But attacks demanding ransom against all U.S. institutions are spiraling higher. The FBI's Internet Crime Complaint Center received 2,673 ransomware reports in the year ending last September — nearly double from 2014.

While manufacturers are increasingly prey to these cyber-stickups, it may just be because criminals are playing the odds and striking as many enterprises of all types as they can across a targeted region, said John Miller, who heads a team at cybersecurity firm FireEye that tracks money-driven online threats.

Attackers "aren't necessarily going after manufacturing to the exclusion of other sectors or with a preference above other sectors. It's more that, 'OK, we're going to try to infect everybody in this country that we can,'" Miller said.

One high-profile example came in May and June, when auto manufacturers including Renault shut down production after they were swept up in the worldwide onslaught of the WannaCry ransomware virus.

But attackers also are increasingly injecting ways to remotely control the robots and other automated systems that control production inside targeted factories.

The threat of computer code tailored to hit specific targets has been around since researchers in 2010 discovered Stuxnet, malware apparently designed to sabotage Iran's nuclear program by causing centrifuge machines to spin out of control. Stuxnet is widely believed to be a covert American and Israeli creation, but neither country has officially acknowledged a role in the attack.

(*Continued On The Following Page)

Malicious software that attacked Ukraine's electricity grid last December was built to remotely sabotage circuit breakers, switches and protection relays, researchers said.

Cyberattacks that reach into industrial control systems have doubled in the past two years in the U.S. to nearly four dozen so far in the federal fiscal year that ends in September, outstripping last year's total, according to DHS data.

"I think the emerging threat you're going to see in the future now is really custom ransomware that's going to be targeted more toward individual companies," said Neil Hershfield, the acting director of the DHS team that handles emergency response to cyberattacks on industrial control systems.

BAE submits bid for SEA 5000

BAE Systems today announced that it has submitted its bid to the Australian Government for the nation's SEA 5000 Future Frigate program.

The bid is to partner with the Government to develop a long-term ship building strategy in Australia for complex warships and to offer a proposal to build nine Anti-Submarine Warfare Frigates for the Royal Australian Navy.

BAE Systems is offering the Global Combat Ship-Australia, a variant of its Type 26 Global Combat Ship which commenced manufacture for the first of three ships for the UK's Royal Navy 20 July.

The campaign is being led by BAE Systems' global Maritime Business Development Director, Nigel Stewart, and the bid was put together by a joint UK and Australian team to ensure the learning and knowledge from the Type 26 program is fully complemented by the maritime skills and expertise of BAE Systems' team in Australia.

Nigel Stewart said: "BAE Systems is proud to have submitted its response to the Australian Government for the SEA 5000 program. By combining the formidable capability of our Type 26 anti-submarine warfare frigate with the heritage and skills we have in Australia, we are sure we can offer a proposition to the Government that is both transformational and compelling. Our commitment is to establish a world class ship building capability in Australia that will build Australian ships with an Australian work force. The opportunity we will bring to Australia through SEA 5000 is unique. It offers us the chance to collaborate across the company by sharing our expertise and experience, transferring embedded knowledge from one market to benefit another.

*(*Continued On The Following Column)*

In addition, BAE Systems is committed to representing Australia in the global marketplace, helping grow Australia's export opportunities and opening up new markets for Australian industry through our global supply chain."

The Type 26 benefits from a modern digital design approach that uses the latest engineering and design technologies. As a fully bow-to-stern digital design, BAE Systems has been able to substantially de-risk construction for the Royal Navy with Australia standing to benefit from all learnings drawn from the UK construction program.

BAE Systems Australia Chief Executive Glynn Phillips said: "BAE Systems has over 3,500 people already working in Australia, a fully mature supply chain of over 1,600 Australian SMEs and we have a proud history of over 60 years working in partnership with the Australian Government as a trusted supplier. Deepening that partnership through selection on SEA 5000 would be a privilege that we are ready and excited to deliver."

Trump Administration Pulls Russian Cyber Firm from Government-Approved List

The Trump administration has decided to remove one of the world's biggest and most-respected cybersecurity firms from the U.S. government's list of companies whose products are approved for use on federal systems, according to U.S. officials.

The decision comes as the Moscow-based company, Kaspersky Lab, faces increasing scrutiny from U.S. officials over alleged ties to Russian intelligence services.

The government list -- known as a schedule -- is maintained by the General Services Administration, and GSA "made the decision to remove Kaspersky Lab-manufactured products" after "review and careful consideration," a GSA spokeswoman said in a statement to ABC News.

"GSA's priorities are to ensure the integrity and security of U.S. government systems and networks and evaluate products and services available on our contracts using supply chain risk management processes," the statement added.

Removing Kaspersky Lab from the General Services Administration's (GSA) list would likely affect only future contracts, ABC News was told.

Classified Senate briefing expands to include Russian cyber firm under FBI scrutiny.

*(*Continued On The Following Page)*

Senate effort to ban Russian software on US military systems would have far-reaching impact, sources say as of Tuesday evening, Kaspersky Lab had not been notified of the decision, according to a company spokeswoman.

For weeks, the White House, the Department of Homeland Security, the GSA and other federal agencies conducted an interagency review of the matter, sources said. And ABC News reported earlier today that the Trump administration was considering such a move.

The final decision to remove Kaspersky Lab from the GSA schedule marks the most significant and far-reaching response yet to concerns among U.S. officials that Russian intelligence services could try to exploit Kaspersky Lab's anti-virus software to steal and manipulate users' files, read private emails or attack critical infrastructure in the United States. The company has repeatedly insisted it poses no threat to U.S. customers and would never allow itself to be used as a tool of the Russian government.

Kaspersky Lab's CEO, Eugene Kaspersky, recently said any concerns about his company are based in "ungrounded speculation and all sorts of other made-up things," adding that he and his company "have no ties to any government, and we have never helped nor will help any government in the world with their cyberespionage efforts."

Nevertheless, the FBI has been pressing ahead with a long-running counterintelligence probe of the company, and in June, FBI agents interviewed about a dozen U.S.-based Kaspersky Lab employees at their homes, ABC News was told. In addition, as ABC News reported in May, the Department of Homeland Security issued in February a secret report on the matter to other government agencies. And three months ago, the Senate Intelligence Committee sent a secret memorandum to Director of National Intelligence Dan Coats and Attorney General Jeff Sessions demanding that the Trump administration address "this important national security issue."

Despite all the private expressions of concern, the issue was first brought into public view only recently by key members of the Senate Intelligence Committee, who began asking questions about Kaspersky Lab during hearings covering global threats to national security.

Lawmakers and other U.S. officials point to Kaspersky Lab executives with previous ties to Russian intelligence and military agencies as reason for concern.

*(*Continued On The Following Column)*

Three weeks ago, Sen. Jeanne Shaheen, D-N.H., took legislative steps to bar the U.S. military from using Kaspersky Lab products.

In a statement Tuesday, she said she was "encouraged" to hear that the Trump administration was potentially "delisting Kaspersky software for use in the federal government." She called it a "wise precaution" that "would work in concert with my [efforts]."

Eugene Kaspersky, however, called those efforts "an extreme new measure."

"Kaspersky Lab is facing one of the most serious challenges to its business yet, given that members of the U.S. government wrongly believe the company or I or both are somehow tied to the Russian government," he recently wrote on his blog.

"Basically, it seems that because I'm a self-made entrepreneur who, due to my age and nationality, inevitably was educated during the Soviet era in Russia, they mistakenly conclude my company and I must be bosom buddies with the Russian intelligence agencies ... Yes, it is that absurdly ridiculous." U.S. officials have yet to publicly present any evidence indicating concerning links between Kaspersky Lab employees and elements of the Russian government.

"Kaspersky Lab believes it is completely unacceptable that the company is being unjustly accused without any hard evidence to back up these false allegations," the company said in a statement today. "Kaspersky Lab, a private company, seems to be caught in the middle of a geopolitical fight where each side is attempting to use the company as a pawn in their political game."

But one senior U.S. intelligence official said the fact that the U.S. government was considering the drastic step of removing Kaspersky Lab from the GSA's list of approved vendors shows that such concerns are "nontrivial."

A company lands on the list after hammering out deals with the GSA, which uses "the government's buying power to negotiate discounted pricing," according to the GSA.

Hundreds of "federal customers" and, in some cases, state and local governments can then purchase the company's products without having to each negotiate their own prices, the GSA said in a 2015 brochure about its operations.

"The buying process is simplified because GSA has completed the bulk of the procurement process on behalf of government buyers," the brochure added. As of a few years ago, the information technology portion of the GSA schedule accounted for more than $14 billion of the federal budget, the brochure said.

*(*Continued On The Following Page)*

An ABC News investigation earlier this year found that — largely through outside vendors — Kaspersky Lab software has been procured by many federal agencies, including the Bureau of Prisons and some segments of the Defense Department.

Kaspersky Lab products are also used in countless American homes and in state and local agencies across the country. "Kaspersky Lab continues to be available to assist all concerned government organizations with any investigations, and the company ardently believes a deeper examination of Kaspersky Lab will confirm that these allegations are unfounded," the company said in its statement today.

Two Iranian Nationals Charged in Hacking of Vermont Software Company

An indictment was unsealed today charging Mohammed Reza Rezakhah, 39 and Mohammed Saeed Ajily, 35, both Iranian nationals, with a criminal conspiracy relating to computer fraud and abuse, unauthorized access to, and theft of information from, computers, wire fraud, exporting a defense article without a license, and violating sanctions against Iran. The court issued arrest warrants for both defendants.

Acting Assistant Attorney General for National Security Dana J. Boente, Acting U.S. Attorney Eugenia A.P. Cowles of the District of Vermont, Assistant Director Scott Smith of the FBI's Cyber Division, and Special Agent in Charge Vadim Thomas of the FBI's Albany, New York Field Office made the announcement.

According to the allegations in the indictment filed in Rutland, Vermont, beginning in or around 2007, Rezakhah, Ajily, and a third actor who has already pleaded guilty in the District of Vermont for related conduct, conspired together to access computers without authorization in order to obtain software which they would then sell and redistribute in Iran and elsewhere outside the U.S. Ajily, a businessman, would task Rezakhah and others with stealing or unlawfully cracking particular pieces of valuable software. Rezakhah would then conduct unauthorized intrusions into victim networks to steal the desired software.

(*Continued On The Following Column)

"Never stop doing your best just because someone doesn't give you credit"

Once the software was obtained, Ajily marketed and sold the software through various companies and associates to Iranian entities, including universities and military and government entities, specifically noting that such sales were in contravention of U.S. export controls and sanctions.

As part of this conspiracy, in October 2012, Rezakhah hacked a Vermont-based engineering consulting and software design company best known for its software that supports aerodynamics analysis and design for projectiles. This software is designated as a "defense article" on the U.S. Munitions List of the International Traffic in Arms Regulations (ITAR), meaning it cannot be exported from the U.S. without a license from the U.S. Department of State. Ajily thereafter promoted the same software as one of the products he could offer to his Iranian clients.

The charges in the indictment are merely accusations, and the defendants are presumed innocent unless and until proven guilty.

The FBI's Albany Cyber Squad investigated the case. The case is being prosecuted by Acting U.S. Attorney Eugenia A.P. Cowles of the District of Vermont and Deputy Chief Sean Newell of the National Security Division's Counterintelligence and Export Control Section. The Justice Department's Office of International Affairs also provided significant assistance in this matter.

Web Notice: The Directorate of Defense Trade Controls (DDTC) is currently in the process of modernizing its IT systems. During this time period, we anticipate there may be delays in response times and time to resolve IT related incidents and requests. We apologize for any inconvenience, and appreciate your patience while we work to improve DDTC services. If you need assistance, please contact the DDTC Service Desk at (202) 663-2838, or email at DtradeHelpDesk@state.gov (06.28.16)