

For Washington, Russian And China Tech Spies Suddenly Everywhere



A Russian 'Orion' long-endurance unmanned aerial vehicle, developed by Aurora Flight Sciences Corp., at the Kubinka airfield in

year.

Today In:

As we are about to enter the final quarter of 2019, it seems a certainty that more of the same can be expected with regards to Russia and China. If it's not tariffs, it's sanctions.

Despite Trump's overtures to both countries, despite his call to bring Russia into the G7 and make it the G8 again, his tenure has been highly antagonizing to the Kremlin. Sanctions on technology sales to Moscow, and even quasi-sanctions on Russia and Chinese nationals working in the U.S., are not going away.

BRANDVOICE

Japan's Blockchain Sandbox Is Paving The Way For The Fintech Future

BRANDVOICE

Tick, Tick, Roth – Why There's Potentially No Better Time To Convert Your IRA To A Roth IRA

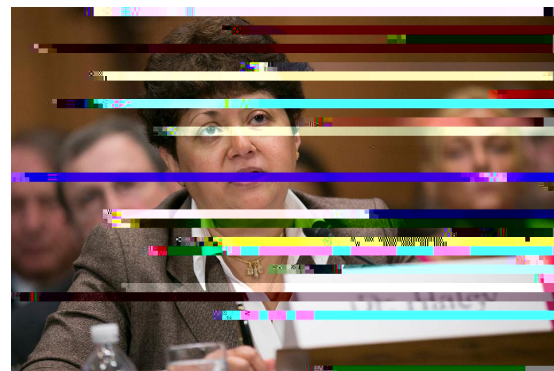
ExtraHop BRANDVOICE

How To Turn Shadow IT Into A Business Asset

“We have the Chinese civilian spy agency hacking private and government servers or using conventional industrial spying by Chinese nationals embedded in U.S. companies already,” says Usha Haley, a professor of management from Wichita State University, who has written extensively on China. Her latest is on China investment in U.S. oil and gas companies in order to gain expertise on fracking technologies.

“The level of theft out of China has increased,” she says, saying nearly two thirds of Department of Justice patent infringement cases involve China. “They don't care if they get caught. They want as much info as they can before the source dries up. I don't know if it will dry up. But right now they see it as fertile ground. They know the U.S. is getting much more cautious about them.”

Last December, two Chinese nationals were



Usha Haley, professor of global business at Wichita State University, at a Senate hearing in 2013 about

industrial espionage efforts, based on cases at the

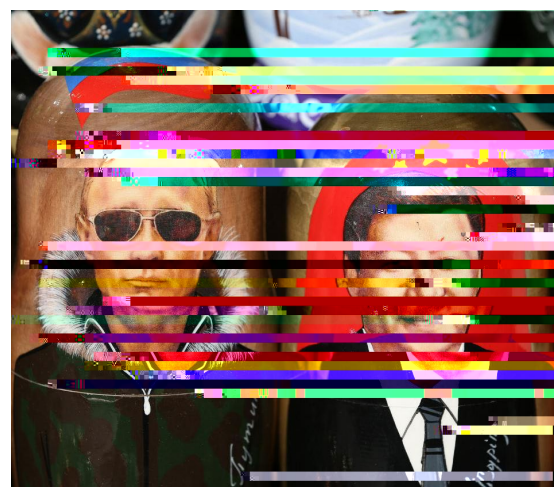
indicted for conspiracy to hack into private servers, commit wire fraud, and identity theft. The two in question worked for Huaying Haitai Science & Technology Development Company and acted in cahoots with the Chinese Ministry of State Security in Tianjin. According to the Pentagon, these guys worked with the Advanced Persistent Threat 10 (APT10) group, conducted global campaigns of hacking, going primarily after U.S. corporate secrets. The APT10 group supposedly stole large amounts of data from aviation companies, space and satellite technology IP, manufacturing technology, computer hardware, pharma, oil and gas, you name it. Companies that were victimized were not mentioned in the report.

The U.S. is in a mild panic over this. If two countries ever stood in the way of the U.S. benign global hegemony it is Russia and China. That's how Washington sees it. If there is to be a one world order led by U.S. corporations and Washington, Russia and China would have to be brought to heel in the opinion of the mainstream American foreign policy makers.

Russia and China are cooperating on military exercises and arms sales and are slowly building links to live in a world of U.S. sanctions. If Washington is ostracizing them, then Moscow and Beijing may join forces. Cold War 2.0 is here.

Sometimes the players are political appointees. With the case of Russia, they jockey in and out of both the government and business.

Former Russian minister of "Open Government" in charge of liaison between then president Dmitry Medvedev and the Russian business class, Mikhail Abyzov, was arrested in March on suspicion of embezzling 4 billion rubles (\$62 million). He faces up to 20 years behind bars if convicted. The ex-minister has denied the charges. He is still waiting for a hearing.



Matryoshka dolls depicting Vladimir Putin and Xi Jinping on display at a souvenir stand in St.

ANDREY RUDAKOV/© 2019

Connected to the Russian

Maria Butinažk \c \YdYXVf]b['h YBU]cbU F]ÚY5ggcV]hcb hc Fi gg]UUbXk UgcbWU
a i W'U_ YXUci hÛ[i fY]b'h YFi gg]UHfi a d'Wbgd]fUW'h Ycfm

Abyzov, a former billionaire, was once the sole shareholder of weapons company called

in 2018 on suspicion of embezzlement, which may be why his picture is not on their website.

The Investigative Committee of Russia, Russia's anti-corruption agency, believes he embezzled \$20 million from the government run Russian Venture Company through a Richmond, California-based portfolio holding called Alion Energy. The company manufactures robots for automatic assembly of solar photovoltaic plants.

A look at their current investments in the U.S shows what type of company Russia venture

Their portfolio includes a \$75 million investment Santa Clara, California-based Alta

Last year, [Alta Devices said](#) the U.S. Navy Research Laboratory would use its devices for some test drones. There is a global competition going on between the U.S., Russia, and China to spearhead the drone-technology development.

Curious Russian investors may want to know what's going on in the U.S. Navy. And their one degree of separation gets Russian hawks in a tizzy.

"You will see some blocking of investment deals involving Russians, especially if it interfaces with the U.S. security community in any way," says Mark Simakovsky, a nonresident fellow at The Atlantic Council's Eurasia Center. Simakovsky worked at the State Department and Pentagon under George W. Bush and Barack Obama between 2007 and 2015.

Some Russian companies are welcome here. *Forbes*-listed billionaire Oleg Deripaska's aluminum company Rusal invested in Kentucky. But even that will get closer due diligence.

Vladimir Putin says the U.S. is playing politics with all this industrial espionage spy "nonsense." ALEXANDER

Twitter or *LinkedIn*

I've spent 20 years as a reporter for the bes in the business, including as a Brazil-based safer for WSJ. Since 2011, I focus on business and invest ing in the big eme... **Read More**

©2019 Forbes Media LLC. All Rights Reserved.
