EIB World Trade Headlines

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

January 2022 - Volume 14, Issue 1

OFAC SANCTIONS UKRAINIAN DESTABILIZERS

January 20, 2022

WASHINGTON – Today, the Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned four individuals engaged in Russian government-directed influence activities to destabilize Ukraine. This is the latest action we have taken to target purveyors of Russian disinformation, including designations in April 2021.

Today's action is intended to target, undermine, and expose Russia's ongoing destabilization effort in Ukraine. This action is separate and distinct from the broad range of high impact measures the United States and its Allies and partners are prepared to impose in order to inflict significant costs on the Russian economy and financial system if it were to further invade Ukraine.

The individuals designated today act at the direction of the Russian Federal Security Service (FSB), an intelligence service sanctioned by the United States, and support Russia-directed influence operations against the United States and its allies and partners. The four individuals have played various roles in Russia's global influence campaign to destabilize sovereign countries in support of the Kremlin's political objectives. The United States will continue to take steps, through actions like this one, and in partnership with the Ukrainian government, to identify, expose, and undercut Russia's destabilization efforts.

"The United States is taking action to expose and counter Russia's dangerous and threatening campaign of influence and disinformation in Ukraine," said Deputy Secretary of the Treasury Wally Adeyemo. "We are committed to taking steps to hold Russia accountable for their destabilizing actions."

*(*Continued On The Following Page)*

NEWSLETTER NOTES

Russian intelligence services, including the FSB, recruit Ukrainian citizens in key positions to gain access to sensitive information, threaten the sovereignty of Ukraine, and then leverage these Ukrainian officials to create instability in advance of a potential Russian invasion. The United States has worked closely with the Government of Ukraine to identify and expose these actors to thwart Russia's influence operations.

In 2020, Kremlin officials launched a comprehensive information operation plan designed in part to degrade the ability of the Ukrainian state to function independently and without Russian interference. This included identifying and co-opting pro-Russian individuals in Ukraine and undermining prominent Ukrainians viewed as pro-Western, who would stand in the way of Russian efforts to bring Ukraine within its control. Goals of the plan included destabilizing the political situation in Ukraine and laying the groundwork for creating a new, Russian-controlled government in Ukraine.

Russia's influence campaigns are not only focused on Ukraine. For over a decade, Russia has employed disinformation outlets and intelligence service affiliates to spread false narratives in support of its strategic goals. Since at least 2016, Russian agents have even sought to influence U.S. elections by spreading disinformation, sowing discord among U.S. audiences, and falsely denigrating U.S. politicians and political parties.

FSB PAWNS IN UKRAINE CONTINUE DESTABILIZATION ACTIVITIES

Russia has directed its intelligence services to recruit current and former Ukrainian government officials to prepare to take over the government of Ukraine and to control Ukraine's critical infrastructure with an occupying Russian force. At the heart of this effort are Taras Kozak (Kozak) and Oleh Voloshyn (Voloshyn), two current Ukrainian Members of Parliament from the party led by Victor Medvedchuk (Medvedchuk), who is already subject to U.S. sanctions for his role in undermining Ukrainian sovereignty in 2014. Medvedchuk maintains close ties with the Kremlin, and also took part in directing these activities.

Kozak, who controls several news channels in Ukraine, supported the FSB's plan to denigrate senior members of Ukrainian President Volodymyr Zelenskyy's inner circle, falsely accusing them of mismanagement of the COVID-19 pandemic. Furthermore, Kozak used his news platforms to amplify false narratives around the 2020 U.S. elections first espoused by U.S.-designated Andrii Leonidovych Derkach (Derkach). Kozak has attempted to legitimatize Derkach's claims by rebroadcasting Derkach's false assertions about U.S. political candidates. Throughout 2020, Kozak worked alongside FSB intelligence agents.

*(*Continued On The Following Column)*

Voloshyn has worked with Russian actors to undermine Ukrainian government officials and advocate on behalf of Russia. Voloshyn also worked with U.S.-designated Konstantin Kilimnik, a Russian national with ties to Russian intelligence who was sanctioned for attempts to influence the U.S. 2020 presidential election, to coordinate passing on information to influence U.S. elections at the behest of Russia. Kozak is being designated pursuant to Executive Order (E.O.) 14024 for being responsible for or complicit in, or for having directly or indirectly engaged or attempted to engage in, interference in a United States or other foreign government election, for or on behalf of, or for the benefit of, directly or indirectly, the Government of the Russian Federation.

Voloshyn is being designated pursuant to E.O. 14024 for having acted or purported to act for or on behalf of, directly or indirectly, the Government of the Russian Federation.

Volodymyr Oliynyk (Oliynyk) is a former Ukrainian official who fled Ukraine to seek refuge in Russia. Oliynyk has a history of supporting Russia, currently resides in Moscow, Russia, and shares Russia's anti-Western sentiments. In 2021, Oliynyk worked at the direction of the FSB to gather information about Ukrainian critical infrastructure.

As in previous Russian incursions into Ukraine, repeated cyber operations against Ukraine's critical infrastructure are part of Russia's hybrid tactics to threaten Ukraine. The overall strategy is designed to pull Ukraine into Russia's orbit by thwarting Ukraine's efforts at Western integration, especially with the European Union (EU) and North Atlantic Treaty Organization (NATO). As Russia has pursued broad cyber operations against critical infrastructure, it has focused on disrupting one critical infrastructure sector in particular: Ukraine's energy sector. Russia has also degraded Ukraine's access to energy products in the middle of winter. Acting through Russia's state-owned gas company Gazprom, Russia has repeatedly disrupted supplies to Ukraine—a vital transshipment country with pipelines to other European countries—due to purported disputes over gas pricing. Oliynyk is being designated pursuant to E.O. 14024 for having acted or purported to act for or on behalf of, directly or indirectly, the Government of the Russian Federation.

Vladimir Sivkovich (Sivkovich) is the former Deputy Secretary of the Ukrainian National Security and Defense Council. In 2021, Sivkovich worked with a network of Russian intelligence actors to carry out influence operations that attempted to build support for Ukraine to officially cede Crimea to Russia in exchange for a drawdown of Russian-backed forces in the Donbas, where separatists continue to receive support from Russia. In early 2020, Sivkovich coordinated with Russian intelligence services to promote Derkach's disinformation campaign against the U.S. 2020 presidential election. Sivkovich, who has ties to the FSB, also supported an influence operation targeting the United States from 2019 to 2020.

(*Continued On The Following Page)

Sivkovich is being designated pursuant to E.O. 14024 for having acted or purported to act for or on behalf of, directly or indirectly, the Government of the Russian Federation.

SANCTIONS IMPLICATIONS

As a result of today's action, all property and interests in property of the designated persons described above that are in the United States or in the possession or control of U.S. persons are blocked and must be reported to OFAC. In addition, any entities that are owned, directly or indirectly, 50 percent or more by one or more blocked persons are also blocked. Unless authorized by a general or specific license issued by OFAC, or exempt, OFAC's regulations generally prohibit all transactions by U.S. persons or within (or transiting) the United States that involve any property or interests in property of designated or otherwise blocked persons. The prohibitions include the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any blocked person, or the receipt of any contribution or provision of funds, goods, or services from any such person.

Background Press Call by a Senior Administration Official on Cybersecurity

January 14, 2022
Via Teleconference
4:33 P.M. EST

MODERATOR: Hey, everyone. Thanks for joining us closer to the end of the day on a Friday. So, as noted in the invite, this is a background call on cybersecurity. I'm going to let our speaker get into more details about that.

Before I turn it over to the speaker, let me just do the ground rules really quickly.

So, this briefing is on background. It is attributable to a "senior administration official." And it is embargoed until the conclusion of the call.

Just for your awareness but not for reporting, the speaker on this call is [senior administration official].

You know, we're running a little bit behind time today, so we're only going to have time for a couple of questions. But if you don't get your question in, you know how to reach me, and I'm happy to get back to you as soon as I can.

So, with that, I'll turn it over to you.

*(*Continued On The Following Column)*

SENIOR ADMINISTRATION OFFICIAL: Thank you very much. And good afternoon, everyone. Like [moderator] said, thank you for joining us late on a Friday afternoon.

So, we welcome, of course, that the Kremlin is taking law enforcement steps to address ransomware emanating from its borders.

The President believes in diplomacy. President Biden and President Putin set up a White House-Kremlin Experts Group on ransomware last June. As we've said and the Russians have acknowledged, we've been sharing information with the Russians through this channel, including information related to attacks on American critical infrastructure.

We understand that one of the individuals who was arrested today was responsible for the attack
against Colonial Pipeline last spring.

We're committed to seeing those conducting ransomware attacks against Americans brought to justice, including those that conducted these attacks on JBS, Colonial Pipeline, and Kaseya.

I also want to be very clear: In our mind, this is not related to what's happening with Russia and Ukraine. I don't speak for the Kremlin's motives, but we're pleased with these initial actions.

We've also been very clear: If Russia further invades Ukraine, we will impose severe costs on Russia in coordination with our allies and partners.

As the President has said, cyber criminals are resilient and we will continue to take action to disrupt and deter them while engaging in diplomacy, as we have with Russia, allies, and partners around the world.
So, with that, over to you. Looking forward to your questions.

Q Thank you so much. Thanks for doing it. I want to ask you about Russia and Ukraine. And I had a little difficulty hearing, but I think you said that if they did anything regarding Ukraine, there would be costs.

Do you have any attribution? I know the Ukrainians have suggested that today's hacking was related to Russian intelligence services. Has this moved beyond what the Pentagon said earlier and what the White House said earlier about attributions about today or any other hacking of Ukraine in recent days from Russia?

SENIOR ADMINISTRATION OFFICIAL: Hi, Andrea. Can you hear me now? I'm sorry. I have a bad cold, so I know I'm a little hard to hear.

Q Oh, I'm so sorry. Feel better.

*(*Continued On The Following Page)*

SENIOR ADMINISTRATION OFFICIAL: Okay. Okay, good. But I'm glad you can hear me. Okay.

So, we don't have an attribution at this time. We are in touch with Ukrainians and have offered our support as Ukraine investigates the impact and recovers from the incident. While we continue to assess the impact to Ukrainians, it seems limited so far, with multiple websites coming back online.

But I want to note, we are — you know, we and our allies and partners are concerned about this cyberattack, and the President has been briefed. But that is the status at this time.

Q Hi. Thank you so much for agreeing to do this on a Friday evening. I was curious to know — you said you welcome reports that the Kremlin is taking action. Obviously, there's been a suggestion that this operation was done at the direct behest of the White House. Could you talk a little bit about whether that's, in fact, true — whether this is something that was done specifically at your urging, with information that the White House had indeed provided? Thank you.

SENIOR ADMINISTRATION OFFICIAL: Thank you, Eric. So, as you know, President Biden and President Putin set up the White House-Kremlin Experts Group on ransomware last June, and we have been meeting within that channel and discussing the need for Russia to take action against ransomware criminals operating from within their borders. We've also shared information regarding individuals operating from within Russia who have conducted disruptive attacks against U.S. critical infrastructure.

And as I noted, we understand that one of the individuals who was arrested today was indeed the individual responsible for the attack against Colonial Pipeline last spring.

So, this has — we do attribute today's announcement to the — to, really, the President's commitment to diplomacy and the channel that he established and the work that has been underway in sharing information and in discussing the need for Russia to take action.

SENIOR ADMINISTRATION OFFICIAL: Okay. Okay, good. But I'm glad you can hear me. Okay.

So, we don't have an attribution at this time. We are in touch with Ukrainians and have offered our support as Ukraine investigates the impact and recovers from the incident. While we continue to assess the impact to Ukrainians, it seems limited so far, with multiple websites coming back online.

But I want to note, we are — you know, we and our allies and partners are concerned about this cyberattack, and the President has been briefed. But that is the status at this time.

*(*Continued On The Following Column)*

Q Hi. Thank you so much for agreeing to do this on a Friday evening. I was curious to know — you said you welcome reports that the Kremlin is taking action. Obviously, there's been a suggestion that this operation was done at the direct behest of the White House. Could you talk a little bit about whether that's, in fact, true — whether this is something that was done specifically at your urging, with information that the White House had indeed provided? Thank you.

SENIOR ADMINISTRATION OFFICIAL: Thank you, Eric. So, as you know, President Biden and President Putin set up the White House-Kremlin Experts Group on ransomware last June, and we have been meeting within that channel and discussing the need for Russia to take action against ransomware criminals operating from within their borders. We've also shared information regarding individuals operating from within Russia who have conducted disruptive attacks against U.S. critical infrastructure.

And as I noted, we understand that one of the individuals who was arrested today was indeed the individual responsible for the attack against Colonial Pipeline last spring.

So, this has — we do attribute today's announcement to the — to, really, the President's commitment to diplomacy and the channel that he established and the work that has been underway in sharing information and in discussing the need for Russia to take action.

That being said, each country pursues its law enforcement operations under, certainly, its own legal system. And Russia's announcement today was clearly something that will be — you know, that was — pursued its own law enforcement steps.

These are our first — these are very important steps, as they represent the Kremlin taking action against criminals operating from within its borders. And they represent what we're looking for with regard to continued activities like these in the future.

Q Hi. Thanks for doing the call. Do you expect anything to happen to these individuals who have been apprehended? As you know, there's no extradition treaty, and Russia has a history of not really prosecuting these types of people. So, what happens now? What does the White House hope to happen now, in terms of actually making sure that these people won't return to ransomware?

SENIOR ADMINISTRATION OFFICIAL: Our expectation is that Russia announce arrests and that Russia would be pursuing legal action within its own system against these criminals for the crimes that they have created — that they have done. So, that is our expectation.

And it is indeed, to your point, our expectation that they're brought to justice and, as such, not only for their past crimes, but preventing future ones as well.

MODERATOR: Thank you. Again, thanks, everyone, for joining. I know this was a really short call. If we didn't get to your question, please feel free to email or call me, and I'll make sure that we get back to you. And then, have a great weekend. Thanks for your time. Bye.

FORT GEORGE G. MEADE, Md.

– The Defense Information Systems Agency (DISA) and the Department of Defense at-large are amidst a global-power competition in an ever-changing cyber landscape with increasing risks and threats from sophisticated adversaries. With the onset of the COVID-19 pandemic, the cyber-attack surface has also intensified as more individuals telework and as more applications and data migrate to the cloud.

In response, DISA has awarded a $6.8M contract to Booz Allen Hamilton for execution of a Thunderdome Prototype, a zero trust security model that aligns with the president's executive order to improve the nation's cybersecurity posture. During this six-month effort, the agency will operationally test how to implement DISA's Zero Trust Reference Architecture, published in March 2020 for DOD, by taking advantage of commercial technologies such as Secure Access Service Edge (SASE) and Software Defined-Wide Area Networks (SD-WAN). Thunderdome will also incorporate greater cybersecurity centered around data protection and integrate with existing endpoint and identity initiatives aligned to zero trust.

"Over the course of the next six months, we plan to produce a working prototype that is scalable across the department," said Jason Martin, director of DISA's digital capabilities and security center. "During that time, we will do what DISA does best – build, test, validate and implement the premier cybersecurity solutions for the Department of Defense and warfighter around the world."

Commerce Department Requests Information on Supporting a Strong U.S. Semiconductor Industry

WASHINGTON – The U.S. Department of Commerce is calling for information that will guide programs designed to support a strong domestic semiconductor industry. The Request for Information published today in the Federal Register asks for input to inform the planning and design of potential programs to incentivize investment in semiconductor manufacturing facilities and associated ecosystems; provide for shared infrastructure to accelerate semiconductor research, development, and prototyping; and support research related to advanced packaging and advanced metrology to ensure a robust domestic semiconductor industry.

"The United States faces both an immediate supply shortage that's driving up prices and a long-term threat to America's economic and national security if we don't increase domestic supply of chips," said Secretary of Commerce Gina M. Raimondo. "As demand for semiconductors will only increase, we need smart, strategic investments to shore up our domestic supply chain – and we need it now.

*(*Continued On The Following Column)*

Not only to address current shortage and supply chain issues but to help position America to lead globally by investing in our semiconductor manufacturing and R&D and enhance American competitiveness."

Semiconductors are fundamental to nearly all modern industrial and national security activities, and they are essential building blocks of other emerging technologies, such as artificial intelligence, autonomous systems, 5G communications and quantum computing. To strengthen the U.S. position in semiconductor R&D and manufacturing, the Biden Administration is seeking full funding for the CHIPS Act programs.

"We urge Congress to pass the President's proposed $52 billion in funding for domestic semiconductor production as part of legislation similar to the U.S. Innovation and Competition Act," Raimondo added. "This much-needed legislation also has funding to incentivize investments in new semiconductor manufacturing facilities in the U.S. as well as billions to establish a National Semiconductor Technology Center."

Congress authorized a set of programs in Title XCIX ("Creating Helpful Incentives to Produce Semiconductors in America") of the William M. (Mac) Thornberry National Defense Authorization Act (NDAA) for Fiscal Year 2021 (Pub. L. No. 116-283). This comprehensive set of programs is intended to restore U.S. leadership in semiconductor manufacturing by providing incentives and encouraging investment to expand manufacturing capacity for the most advanced semiconductor designs, as well as those of more mature designs that are still in high demand.

These programs would also support growth of the research and innovation ecosystem for microelectronics and semiconductor R&D in the U.S., including investments in the infrastructure necessary to better integrate advances in research into semiconductor manufacturing.

The U.S. semiconductor industry has historically dominated many parts of the semiconductor supply chain, such as research and development (R&D), chip design and manufacturing. Over the past several years, the U.S. position in the global semiconductor industry has faced numerous challenges. In 2019, the United States accounted for 11% of global semiconductor fabrication capacity, down from 13% in 2015 and continuing a long-term decline from around 40% in 1990. Much of the overseas semiconductor manufacturing capacity is in Taiwan (led by Taiwan Semiconductor Manufacturing Company), South Korea (led by Samsung), and, increasingly, China.

The Department of Commerce published the RFI to seek input on a potential set of programs in general and the following topics specifically:

*(*Continued On The Following Page)*

- A semiconductor financial assistance program that would provide funding, through a competitive process, to private entities, consortia of private entities, or public-private consortia to incentivize the establishment, expansion, or modernization of semiconductor manufacturing facilities and supporting infrastructure.
- A National Semiconductor Technology Center to serve as a hub of talent, knowledge, investment, equipment and toolsets.
- An advanced packaging manufacturing program that focuses on the challenge of embedding fragile computer chips into very small configurations that combine multiple systems resulting in benefits including lower costs, increased functionality and improved energy efficiency.
- The current and future workforce development needs of the semiconductor industry.

DOC may hold workshops to explore in more detail questions raised in the RFI and will announce any workshop dates and registration deadlines on www.nist.gov/semiconductors.

Comments are invited from all interested parties, domestic or foreign, including semiconductor manufacturers; industries associated with or that support the semiconductor industry, such as materials providers, equipment suppliers, manufacturers and designers; trade associations, educational institutions and government entities; original equipment manufacturers; semiconductor buyers; semiconductor industry investors; and any other stakeholders.

Comments should be submitted via regulations.gov (DOC-2021-0010) by 5 p.m. Eastern time on March 25, 2022.

South Florida Residents Sentenced for Illegally Exporting Controlled Items to Libya

Two Florida residents were sentenced yesterday for conspiring to and illegally attempting to export controlled items to Libya.

Peter Sotis, 57, of Delray Beach, and Emilie Voissem of Sunrise, were convicted in October 2021 following a one-week jury trial in Miami. Sotis was sentenced to 57 months in prison, and Voissem was sentenced to a split sentence of five months in prison and five months of home confinement.

According to court documents, the charges stem from the defendants' scheme to cause the illegal export of rebreather diving equipment to Libya in August 2016. Rebreathers enable a diver to operate undetected for long periods of time underwater by producing little to no bubbles and by efficiently re-circulating the diver's own breath after replacing its carbon dioxide with oxygen. Because of these enhanced capabilities, rebreathers have a dual use, with both civilian and military applications, and are specifically included on the Commerce Control List, which is the list of dual use items that are export controlled and licensed by the U.S. Department of Commerce (DOC). Such restricted items require a Commerce Department license if the rebreathers are to be exported to any countries with national security concerns, such as Libya.

Sotis was the 80% owner of Add Helium, a diving equipment and training company in Fort Lauderdale, Florida, and Voissem was the Add Helium office manager. The defendants were warned that it was illegal to export the items to Libya without a DOC license and they willfully attempted to export those items after receiving an instruction from a DOC special agent that such items were detained and not to be exported while a license determination was pending. The exhibits and testimony at trial showed that the defendants lied to and misled Ramas LLC, a shipping company in Virginia, about what the DOC agent had told them and about whether the rebreathers had a military use. Testimony at trial also showed that Sotis threatened a government witness not to cooperate with the federal investigation.

Assistant Attorney General Matthew G. Olsen of the Justice Department's National Security Division; U.S. Attorney Juan Antonio Gonzalez for the Southern District of Florida; Special Agent in Charge Ariel Joshua Leinwand of the DOC's Office of Export Enforcement Miami Office; and Special Agent in Charge Anthony Salisbury of the U.S. Immigration and Customs Enforcement's Homeland Security Investigations' (HSI) Miami Office made the announcement.

DOC and HSI investigated the case with valuable assistance provided by the FBI's Miami Field Office and the U.S. Customs and Border Protection.

*(*Continued On The Following Page)*

This case was prosecuted by Assistant U.S. Attorneys Michael Thakur and Andy Camacho of the Southern District of Florida, and Trial Attorney Nathan Swinton of the National Security Division's Counterintelligence and Export Control Section.

Topic(s):
Counterintelligence and Export Control
National Security
Component(s):
Federal Bureau of Investigation (FBI)
National Security Division (NSD)
USAO - Florida, Southern

Joint United States – United Kingdom Statement on Addressing Global Steel and Aluminum Excess Capacity

WASHINGTON – United States Secretary of Commerce Gina M. Raimondo, United States Trade Representative Katherine Tai and United Kingdom Secretary of State for International Trade Anne-Marie Trevelyan today announced the start of bilateral discussions to address global steel and aluminum excess capacity, including the United States' application of tariffs on imports from the United Kingdom under Section 232 and the UK's retaliatory tariffs on certain U.S. exports to the UK. Both parties are committed to working towards an expeditious outcome that ensures the viability of steel and aluminum industries in both markets against the continuing shared challenge of global excess capacity and strengthens their democratic alliance.

During a virtual meeting today, Secretary Raimondo and Secretary of State Trevelyan discussed the impact on their industries stemming from global excess capacity driven largely by China. The distortions that result from this excess capacity pose a serious threat to market-oriented steel and aluminum industries in the United States and the United Kingdom, and to the workers in those industries. They agreed that, as the United States and the United Kingdom are close and long-standing partners, sharing similar national security interests as democratic market economies, they can partner to promote high standards, address shared concerns and hold countries that practice harmful market-distorting policies to account.

Secretary Raimondo, Ambassador Tai and Secretary Trevelyan will enter into discussions on the mutual resolution of concerns in this area that addresses steel and aluminum excess capacity and the deployment of effective solutions, including appropriate trade measures, to preserve our critical industries.

Export Control Classification Number 0Y521 Series Supplement—Extension of Controls on an Emerging Technology (Software Specially Designed To Automate the Analysis of Geospatial Imagery Classification)

On January 6, 2020, the Bureau of Industry and Security (BIS) amended the Export Administration Regulations (EAR) to add Software Specially Designed to Automate the Analysis of Geospatial Imagery to the 0Y521 Temporary Export Control Classification Numbers (ECCN) Series as 0D521. BIS first extended controls on this emerging technology for a second year pursuant to the 0Y521 series extension procedures on January 6, 2021, and in this action extends these controls a second time for an additional year for a total of three years of this control since it was added to the EAR on January 6, 2020.

Information Security Controls: Cybersecurity Items; Delay of Effective Date

On October 21, 2021, the Bureau of Industry and Security (BIS) published an interim final rule that establishes new controls on certain cybersecurity items for National Security (NS) and Anti-terrorism (AT) reasons, along with a new License Exception, Authorized Cybersecurity Exports (ACE), that authorizes exports of these items to most destinations except in the circumstances described in that rule. That rule was published with a 45-day comment period, which ended on December 12, 2021, and a 90-day delayed effective date (January 19, 2022). This rule delays the effective date of the interim final rule by 45 days (March 7, 2022). This action does not extend or reopen the comment period for BIS's previous request for comments on the interim final rule.

"Quishing"

As if we needed yet another word to add to our vocabulary, a new one has surfaced: "Quishing". The word is used to describe the use of malicious QR barcodes within phishing emails. A QuickResponse (aka: QR) code is typically displayed as a B&W box image that contains "squiggly" lines that contain locator/website address information that. QR code use has grown exponentially as smartphones replace traditional computer use. Hackers are now using quishing to target cloud-based logon credentials to then further exploit for ransomware or malware attacks

NCSC warns industry, academia of foreign threats to their intellectual property

Russia and China continue to engage in IP theft to bolster their defense technology and economic standing, respectively. The National Counterintelligence and Security Center urges action.

CISOs of companies both small and large understand how intellectual property (IP) and company infrastructure may be targeted from one of four vectors: malevolent insiders, unscrupulous competitors, criminals, or nation states. While ransomware attacks emphasize how criminals monetize their ability to socially engineer individuals to click that link or attachment, nation states are quietly working to fleece the IP and gain foothold within targets of interest.

The U.S. National Counterintelligence and Security Center (NCSC—an entity within the Office of the Director of National Intelligence) recently published a ten-page primer on the targeting of emerging U.S. technologies by these foreign threats. The primer cites artificial intelligence, the bioeconomy, autonomous systems, quantum information science and technology, and semiconductors as key sectors being targeted by foreign adversaries. But by no means are those the only sectors being targeted.

The NCSC first points their finger at both China and Russia, who view these sectors as a national security priority. China's desire to globally dominate these sectors by 2030 is not a secret. Russia is focused on access to the technologies for its military industrial complex.

https://www.csoonline.com/article/3641972/ncsc-warns-industry-academia-of-foreign-threats-to-their-intellectual-property.html

Even on US Campuses, China Cracks Down on Students Who Speak Out

This story was originally published by ProPublica.

Students and scholars from China who criticize the regime in Beijing can face quick retaliation from fellow students and Chinese officials who harass their families back home. U.S. universities rarely intervene.

On the bucolic campus of Purdue University in Indiana, deep in America's heartland and 7,000 miles from his home in China, Zhihao Kong thought he could finally express himself.

In a rush of adrenaline last year, the graduate student posted an open letter on a dissident website praising the heroism of the students killed in the Tiananmen Square massacre in 1989.

The blowback, he said, was fast and frightening. His parents called from China, crying. Officers of the Ministry of State Security, the feared civilian spy agency, had warned them about his activism in the United States.

"They told us to make you stop or we are all in trouble," his parents said.

Then other Chinese students at Purdue began hounding him, calling him a CIA agent and threatening to report him to the embassy and the MSS.

Kong, who goes by the nickname Moody, had already accepted an invitation from an international group of dissidents to speak at a coming online commemoration of the Tiananmen massacre anniversary. Uncertain if he should go through with it, he joined in rehearsals for the event on Zoom.

https://www.moneylife.in/article/even-on-us-campuses-china-cracks-down-on-students-who-speak-out/65737.html

U.S. universities retain ties to Chinese universities that support Beijing's military buildup, new report says

Dec. 10, 2021, 12:00 PM EST / Updated Dec. 14, 2021, 2:55 PM EST By Dan De Luce

Dozens of U.S. universities maintain ties to Chinese universities that conduct defense research in support of Beijing's military buildup, including work related to the country's nuclear weapons program, according to a new report released Thursday.

The partnerships are part of a broader effort by China to leverage its access to U.S. research institutions to acquire technology and knowledge that could benefit its expanding military, according to the report by the Foundation for Defense of Democracies think tank. But the relationships are entirely legal and American universities often tout their ties to "sister" Chinese universities as an academic strength, providing students and scholars with an educational opportunity to collaborate and learn about Chinese language and culture.

The think tank report does not provide new evidence that U.S. universities have failed to safeguard sensitive, national security-related research, but it argues that policy makers and university administrators need to take a closer look at relationships with Chinese universities linked to Beijing's military-industrial complex. The U.S. government should establish "legal and regulatory guardrails to neutralize China's ability either to acquire foundational knowledge or to access more sensitive research being conducted on U.S. college campuses," the report said. China was focused not only on classified or sensitive material but all relevant information that could bolster its military and technological might, said Craig Singleton, the report's author.

"While the U.S. government often twists itself into knots determining what is classified or unclassified, the Chinese government often sees little-to-no distinction. Instead, Beijing is focused on collecting and harnessing any and all useful information to power its defense modernization," Singleton said. "This includes everything from foundational knowledge taught on U.S. college campuses to cutting edge research, much of which is not technically classified but still has potential military applications."

China's embassy in the U.S. rejected the accusation that Beijing was trying to exploit academic cooperation between U.S. and Chinese universities.

https://www.nbcnews.com/politics/national-security/us-universities-retain-ties-chinese-schools-support-chinas-military-bu-rcna8249

China's state-sponsored industrial espionage is part of a larger system

Chinese intelligence officer Yanjun Xu is awaiting sentencing in federal court after he was convicted of attempted theft of trade secrets and economic espionage last month. The U.S. government charged him with trying to steal sensitive engine technology from a U.S. aviation company by extracting information from an employee.

Xu's purpose, intelligence officials say, was to hand that technology over to a Chinese company that the Chinese government hopes could rival Airbus and Boeing.

Xu is the first Chinese intelligence officer extradited to the U.S. to stand trial for espionage, according to the Department of Justice. (He was arrested in Belgium.) But U.S. prosecutors have been accusing Chinese spies of stealing trade secrets for years.

The list of victims is long: solar and steel companies, makers of computer chips and airplanes, labs doing COVID-19 research, health care companies, universities — it goes on and on.

"And it is most certainly guided by the Chinese government," said Michael Orlando, acting director of the National Counterintelligence and Security Center, a government agency that focuses on threats from foreign powers.

"China has a number of national plans, which include Made in China 2025 and their 14th five-year plan, which lists about 10 technologies that they are seeking to dominate in," he said.

These include technologies upon which the industries and wealth generators of the future depend, like artificial intelligence, quantum information systems, biotech, semiconductors and autonomous systems.

"The Chinese government is using all instruments of national power, from espionage to legal acquisitions and joint ventures to acquire specific technologies, so they can be the world leaders in those technologies," Orlando said, adding that China's government will use whatever means necessary — legal and illegal.

That has been plain to see for Mark Widmar. He's CEO of First Solar, the only large-scale U.S. solar cell manufacturer to survive competition from China's — at one point — highly subsidized solar industry.

*(*Continued On The Following Page)*

First Solar uses a specialized technology for its solar panels that Chinese companies do not have and are, he said, trying to acquire one way or another.

“We spend a lot of time around cybersecurity because we are constantly being attacked, and we know a lot of the efforts are being done with companies in China to get access to our data and our information,” Widmar said.

At the same time, Chinese companies are using more above-board methods, as well.

“I have been approached by Chinese associates requesting us to manufacture in China, and they have highlighted benefits they would be willing to provide around subsidies, not having to pay for buildings, highly subsidized capital and other benefits they would provide,” he said.

Despite the allure, Widmar’s refused. “Because we don’t want to expose our technology to potential risk of theft, so we’ve stayed away from manufacturing in China, and that’s one thing that’s helped us.”

China views national security and economic security as one and the same, said Anna Puglisi, director of biotechnology programs and senior fellow at Georgetown University’s Center for Security and Emerging Technology.

“China really looks at development of science and technology as zero-sum,” she said. “That’s really the driver behind a lot of the activities that we see.”

The importance of this is understood at the highest levels, Puglisi said. In a National Development and Reform Commission report from 2017, “[Chinese President Xi Jinping] describes science and technology as a national weapon, that if China wants to be strong, it must have a powerful science and technology,” she said.

Xi has repeated similar language in a more recent speech, where he called science and technology “a sharp weapon for development” and said that “if science and technology are strong, the country will be strong.”

When it comes to sensitive technologies, the relationship between Chinese firms and their government is different than in economies like the United States, Korea, Japan or Europe. Chinese firms can ask specialized “science and technology diplomats” to help them connect with foreign companies that have the technology they need, Puglisi said. “And [those diplomats] help and try and broker those kinds of arrangements and collaborations or business deals.”

*(*Continued On The Following Column)*

“Nonmarket decision-making and state subsidies give unfair advantage to China’s companies and forces U.S. and other Western companies to have to make concessions and give up technology they do not have to do other places in the world,” Puglisi said.

In one example of alleged forced technology transfer on American soil, several former executives of aviation startup Icon Aircraft — including former Boeing CEO Philip Condit — argued in a lawsuit that Chinese majority shareholders lifted Icon’s intellectual property on design and manufacturing.

Chinese firms can also ask China’s intelligence services for help, said Roy Kamphausen, president of the National Bureau of Asian Research and executive director of the Commission on the Theft of American Intellectual Property.

“Can you imagine if a major American company could say to the U.S. government, ‘Hey we’re entering into negotiations with a partner in X, Y, Z country, can the CIA help answer these questions about this company’s operations and trade secrets?’ Even as you say those words, it’s ridiculous, but it’s a very real thing that’s happening,” Kamphausen said.

He and intelligence officials say hacking — like the cyberattacks First Solar endures — have been a powerful tool used by China’s government to extract technology and economic advantage from foreign companies.

“Well, it’s massive, we’ll start with that,” said Adam Meyers, senior vice president of intelligence at CrowdStrike, a cybersecurity firm.

In 2015, U.S. President Barack Obama, Xi Jinping by his side, announced an agreement between the two leaders that neither country would “conduct or knowingly support cyber-enabled theft of intellectual property” for commercial gain.

China has not lived up to that commitment, and in a recent report, CrowdStrike called it “one of the most prolific state-sponsored cyber actors on the planet,”

Cyberattacks launched by any of the 51 groups in China tracked by CrowdStrike — including groups associated with the People’s Liberation Army, the Ministry of State Security and Public Safety, as well as regional intelligence services — map closely to China’s stated ambitions for industries and technologies the government wants its country to dominate, Meyers said.

“There’s just a huge shopping list,” he said. And the attacks have been evolving, Meyers added.

They now go after not only individual companies but the services those companies use, like telecom companies, as a portal to multiple targets.

(*Continued On The Following Page)

"They're using the information they're gleaning from attacks against telecoms to enable going after other targets that might be using those telecoms, businesses or enterprises hosting on telecoms," he said. Meyers said China's government has been at this for decades, with a long-term vision.

"Western businesses are thinking quarter-to-quarter, not 10 to 15 years down the road, which is where Chinese companies are," he said. "They're willing to wait until 2049. They are patient, and that's their secret weapon." China's embassy did not respond to a media inquiry for this story. In public comments, officials have called these kinds of allegations fabrications.

It's hard to estimate the cost of this technology transfer to the U.S. economy through hacking, theft of intellectual property, knockoff products and other means. But Kamphausen at the IP commission has tried.

"It's as large as $600 billion a year. The best studies estimate that for [Organization for Economic Cooperation and Development] countries, trade secret theft alone is between 1% and 3% of GDP. And no matter how you measure it, and no matter the type of IP theft from trade secret theft, counterfeiting, software copying, no matter how you count it," he said China is inflicting 60% to 80% of the damage.'

Five Eyes issue joint advisory for defending against Log4Shell

Government agencies in the United States, United Kingdom, Australia, Canada, and New Zealand—which make up the "Five Eyes" intelligence alliance—issued a joint Cybersecurity Advisory Wednesday offering guidance for those affected by serious vulnerabilities, including Log4Shell, in the widely used Apache Log4j software library.

The problems can allow attackers to remotely execute code on vulnerable systems—which researchers say nation-state and ransomware gangs are already exploiting.

*(*Continued On The Following Column)*

"Don't be busy, be productive."

In a press release accompanying the advisory, U.S. Cybersecurity and Infrastructure Security Agency (CISA) director Jen Easterly described the Log4j vulnerabilities as "the most severe" she's seen in her career and emphasized the global nature of the risk.

"CISA is working shoulder-to-shoulder with our interagency, private sector, and international partners to understand the severe risks associated with Log4j vulnerabilities and provide actionable information for all organizations to promptly implement appropriate mitigations," she said.

The new guidance expands on advice previously released by CISA and its Joint Cyber Defense Collaborative (JCDC), with a focus on securing traditional IT and cloud vendor-based networks as well as operational and industrial control systems.

The advisory covers:

Identifying assets affected by Log4Shell and other Log4j-related vulnerabilities,

Upgrading Log4j assets and affected products to the latest version as soon as patches are available and remaining alert to vendor software updates, and

Initiating hunt and incident response procedures to detect possible Log4Shell exploitation.

Last week, CISA issued an "emergency directive" ordering federal agencies to address Log4j vulnerabilities and on Tuesday the Department of Homeland Security announced it was expanding its bug bounty program to include reports of related issues.