June 5, 2023

First Cases From DOJ's Disruptive Technology Strike Force Cover Export Control Evasion and Trade Secret Theft

On May 16, 2023, the Department of Justice ("DOJ") announced the first five criminal cases brought by its recently created Disruptive Technology Strike Force ("DTSF"),[1] an interagency initiative led by DOJ and the Department of Commerce ("DOC").[2] As we have previously discussed, the aim of the DTSF is to prevent national security threats arising from authoritarian countries' growing technological capabilities. These threats include cyber attacks by nation states or criminal groups supported by nation states; the weaponization of personal data; and the general disruption of private sector, military, and critical public infrastructure.[3]

The five cases brought by different U.S. Attorneys' offices target schemes to steal sensitive U.S. technologies and provide them to foreign companies and governments. Two of the cases, *United States* v. *Li* (C.D. Cal) and *U.S.* v. *Wang* (N.D. Cal.), involve the theft of trade secrets and other technologies related to manufacturing nuclear submarines, military aircraft, and autonomous vehicles to benefit the Chinese government and Chinese companies. Two others, *United States* v. *Bogonikolos* (E.D.N.Y.) and *United States* v. *Besedin and Patsulya* (D. Ariz.), concern efforts to smuggle advanced electronics, battlefield equipment, and aircraft parts to Russia, in violation of export controls related to the invasion of Ukraine. And the fifth, *United States* v. *Xiangjiang Qiao* (S.D.N.Y.), involves an employee of a sanctioned Chinese company who arranged to supply isostatic graphite to Iran for use in developing weapons of mass destruction.

Key Takeaways

The DTSF will focus on corporate espionage, as well as violations of export controls and cyberattacks. When the DTSF was announced, the Deputy Attorney General said its "work will focus on investigating and prosecuting criminal violations of export laws" and "enhancing administrative enforcement of U.S. export controls."[4] Yet two of the five cases announced this month involved individual employees charged with theft of trade secrets from their U.S. employer for the benefit of Chinese companies, rather than any violations of export laws themselves. Grouping those cases with the other three announced at the same time, which involve more traditional export control violations, shows that the U.S. government views a wide range of efforts to obtain U.S. technology as a serious threat to the country. It also demonstrates the DOJ's continued focus on perceived threats from China, even where the government of that country is not directly linked to the alleged crimes.

[1] Dep't of Justice, "Justice Department Announces Five Cases as Part of Recently Launched Disruptive Technology Strike Force" (May 16, 2023) ("DOJ DTSF Case Announcement"), available here.

[2] Dep't of Justice, "Justice and Commerce Departments Announce Creation of Disruptive Technology Strike Force" (Feb. 16, 2023), available here.

[3] Paul, Weiss Client Memorandum, Deputy Attorney General Announces Creation of Disruptive Technology Strike Force (Mar. 3, 2023), available here.

[4] Dep't of Justice, "Justice and Commerce Departments Announce Creation of Disruptive Technology Strike Force," (Feb. 16, 2023), available here.

Insider threats pose significant risks to sensitive technology and intellectual property. Recent DOJ prosecutions aside from the DTSF have focused on the threat posed by insiders.[5] The DTSF cases announced recently further highlight the risks that corporate insiders pose to intellectual property and sensitive technology. For example, in *Li*, the defendant allegedly downloaded corporate files related to the manufacture of nuclear submarines and aircraft from a company device to a personal external hard drive,[6] and in *Wang*, the defendant allegedly stole trade secrets from a U.S. company using his access to a corporate network.[7] Companies involved in developing technology that would be valuable for foreign companies or governments should reassess whether they have sufficient measures in place to prevent the theft of such technology by insiders.

Financial institutions must remain vigilant over transactions related to sensitive technologies. Three of the five DTSF cases involve the use of shell entities to carry out the schemes at issue to evade controls involving sensitive technologies: *Bogonikolos* (wire fraud conspiracy and smuggling), *Besedin and Patsulya* (conspiracy to commit money laundering conspiracy and to violate the Export Control Reform Act) and *Xiangjiang Qiao* (money laundering, bank fraud, and sanctions evasion). The financial aspects of these transactions call to mind that, in June 2022 and May 2023, the Department of Treasury and DOC issued advisories encouraging financial institutions to monitor for and file SARs regarding suspected export control evasion, particularly in light of the increased export controls relating to Russia.[8] In the recent May 2023 advisory, the agencies reminded financial institutions to remain "vigilant" and highlighted "nine high priority Harmonized System (HS) codes" and "additional transactional and behavioral red flags" that they may use to identify attempted export control evasion related to Russia.[9] The high-priority HS codes include electronic integrated circuits (processors and controllers, memories, and amplifiers) and machines for the reception, conversion, and transmission or regeneration of voice, images, or other data.[10] The red flags include "[a] new customer whose line of business is in trade of products associated with the nine HS codes, is based in a non-GECC country, and was incorporated after February 24, 2022" and when "[a] customer lacks or refuses to provide details to banks, shippers, or third parties, including about end users, intended end-use, or company ownership."[11]

The Cases

United States v. *Wang* (N.D. Cal.)

The ND Cal indictment charges a former software engineer at a major U.S. technology company, Weibao Wang, with theft of trade secrets. Wang specialized in the development of software for autonomous systems, and, over the four months before he resigned from the company, secretly accepted a position as an engineer with a U.S.-based subsidiary of a company headquartered in China that was developing self-driving cars, and possibly other autonomous systems.[12] Wang did not disclose during his exit interview where he was planning to work.[13] After Wang left the U.S. company, personnel "reviewed access logs

[5] Paul, Weiss Client Memorandum, Recent DOJ Prosecutions Underscore the Risk from "Insider" Cyber Threats (Apr. 28, 2023), available here.

[6] *United States* v. *Li*, No. 23-00223 ¶ 7 (C.D. Cal. May 5, 2023) (Complaint), available here.

[7] *United States* v. *Wang*, No. 23-104 ¶ 12 (E.D.N.Y. Apr. 11, 2013) (Indictment), available here.

[8] U.S. Dep't of Treasury, *FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Increased Vigilance for Potential Russian and Belarusian Export Control Evasion Attempts*, FIN-2022-Alert003 (June 28, 2022), available here; U.S. Dep't of Treasury, *Supplemental Alert: FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Continued Vigilance for Potential Russian Export Control Evasion Attempts*, FIN-2023-Alert004 (May 19, 2023), available here. *See also* Paul, Weiss 2022 Year in Review, Economic Sanctions and Anti-Money Laundering Developments (Mar. 1, 2023), available here.

[9] U.S. Dep't of Treasury, *Supplemental Alert: FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Continued Vigilance for Potential Russian Export Control Evasion Attempts*, FIN-2023-Alert004 at 1-2 (May 19, 2023), available here.

[10] *Id.* at 7.

[11] *Id.* at 9.

[12] *Wang*, No. 23-104 ¶ 11 (N.D. Cal. Apr. 11, 2013) (Indictment), available here.

[13] *Id.* ¶ 10.

documenting historical activity on [the company's] network" which "identified Wang as having accessed large amounts of sensitive Project information in the days leading up to his departure."[14] When law enforcement searched his residence on June 27, 2018, agents recovered several personal devices containing confidential, proprietary materials related to the U.S. company's development of autonomous systems.[15] Despite telling agents during the search he had no plans to travel, Wang purchased a one-way ticket to Guangzhou, China that same day at 8:34 p.m., and he subsequently boarded that flight at 11:55 p.m.[16]

***United States* v. *Bogonikolos* (E.D.N.Y.)**

The EDNY complaint charges Dr. Nikolas "Nikos" Bogonikolos, the head of a NATO defense contractor that had recently been a finalist in a 2021 NATO Innovation Challenge for the use of "Artificial Intelligence and Blockchain Technology for the safety of space assets like satellites, spacecrafts, etc," with wire fraud conspiracy and smuggling charges.[17] The charges relate to Dr. Bogonikolos' alleged smuggling of U.S.-origin technology to Russia since 2017. According to the DOJ, after Bogonikolos met with a Russian company in Moscow, he falsified export licenses, ordering sophisticated equipment and representing that it would be used by his company in NATO countries, although it was being reshipped and diverted to Russia. In one text message, Bogonikolos explained "I sign that the items are only for Netherlands :)."[18] He was arrested in Paris on May 9, 2023 and is awaiting extradition.

***United States* v. *Li* (C.D. Cal.)**

The CD Cal charged a California man, Liming Li, with theft of trade secrets. Li worked for two California-based software companies and allegedly stole sensitive technology that could be used in the manufacture of nuclear submarines and military aircraft for use by his own business in China. That technology was subject to export controls on national security, nuclear proliferation, and anti-terrorism grounds. According to the DOJ, security at the second company discovered that Li was "using his company-issued laptop to download files from [its] root directory onto his personal external hard drive" and even found a folder labeled "ChinaGovernment" on his company-issued laptop.[19]

Moreover, shortly before Li joined the second company in 2018, Li and his wife had created a "smart manufacturing company" through which prosecutors allege Li planned "to participate in the [People's Republic of China's] Thousand Talents Program," and "provide to PRC business and government entities export-controlled and trade secret technology."[20] Indeed, just a few short months after being terminated from that company, Li was hired by a manufacturing company based in China to help the company develop software for smart manufacturing.[21] Li was arrested while flying back from China.[22]

***United States* v. *Xiangjiang Qiao* (S.D.N.Y.)**

In the SDNY, Chinese national Xiangjiang Qiao was charged with sanctions evasion, money laundering, and bank fraud. The company that Qiao works for, Sinotech Dalian Carbon and Graphic Manufacturing, has been subject to sanctions for providing

[14] *Id.* ¶ 12.

[15] *Id.* ¶ 15.

[16] *Id.* ¶ 13.

[17] *United States* v. *Bogonikolos*, No. 23-412 ¶ 5 (E.D.N.Y. May 2, 2023) (Affidavit and Complaint), available here.

[18] *Id.* ¶ 18.

[19] *Li*, No. 23-00223 ¶ 7 (C.D. Cal. May 5, 2023) (Complaint), available here.

[20] *Id.* ¶ 6-7; DOJ DTSF Case Announcement, available here.

[21] *Id.* ¶ 7.

[22] Id. ¶ 10.

material used in Iran's development of weapons of mass destruction since 2014.[23] Qiao himself is alleged to have "used a bank account in the name of a front company to conceal the role of Sinotech Dalian in the transactions for the sale of isostatic graphite," which is used on the nose tips of intercontinental ballistic missiles, that Qiao believed was destined for an Iranian entity.[24] Qiao is at large in China.

***United States* v. *Besedin and Patsulya* (D. Ariz.)**

The Arizona complaint charges two Russian nationals living in Florida with conspiracy to violate export controls and conspiracy to commit international money laundering. As alleged, the two would "field[ ] requests and orders for parts from various Russian airlines," which had been subject to increased exports controls after the Russian invasion of Ukraine, and "falsely represent[ ] to U.S. suppliers and customs and law enforcement officials that their customers were entities other than Russian airlines, such as companies operating out of Turkey."[25] The two had traveled to Arizona as part of the scheme, where one of the several American companies the pair ordered airplane parts from were located, and they were arrested.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

H. Christopher Boehning
+1-212-373-3061
cboehning@paulweiss.com

Jessica S. Carey
+1-212-373-3566
jcarey@paulweiss.com

John P. Carlin
+1-202-223-7372
jcarlin@paulweiss.com

David Fein
+44-20-7367-1608
dfein@paulweiss.com

Michael E. Gertzman
+1-212-373-3281
mgertzman@paulweiss.com

Roberto J. Gonzalez
+1-202-223-7316
rgonazalez@paulweiss.com

Richard S. Elliott
+1-202-223-7324
relliott@paulweiss.com

David K. Kessler
+1-212-373-3614
dkessler@paulweiss.com

Law clerk Marissa A. Piccolo contributed to this Client Memorandum.

[23] *United States* v. *Xiangjiang Qiao*, No. 23-239 ¶ 2 (S.D.N.Y.) (Indictment), available here.

[24] *Id.* ¶ 3.

[25] *United States* v. *Besedin and Patsulya*, No. 23-3233 ¶ 3 (D. Ariz. May 11, 2023) (Statement of Probable Cause), available here.