An Unfair ADVANTAGE

The United States is facing an unprecedented wave of attempts to obtain intellectual property and trade secrets. Nearly all of them are coming from China.

Hongjin Tan had a good job. A Chinese national and U.S. legal permanent resident, he was employed as an associate scientist for a U.S. petroleum company to work with a team developing the next generation of battery technologies for stationary energy storage.

But after just over two years at the company, Tan contacted his supervisor on 12 December 2018 to give his two weeks' notice. Tan said he wanted to return to China because, as an only child, he needed to be there to care for his aging parents. He did not have a job lined up back home but was in negotiations with a few battery companies about a position.

After Tan gave his notice, the company—following security procedures—revoked his access to company systems and reviewed his recent computer activity. What it found was concerning.

Tan had accessed hundreds of corporate files, including reports on how to make a specific product and the plans to market that product in China. The information was considered a trade secret and outside the data Tan needed access to for his job. The review also found that Tan downloaded restricted

ILLUSTRATION BY LJ DAVIDS

files outside of his scope of work to a personal thumb drive, without authorization.

The company escorted Tan from the property after the review and banned him from returning. Later that same evening, Tan texted his former supervisor, admitting that he had a USB drive with lab data on it that he had been planning to write a report on from his home. He was asked to return the drive, which he did. The drive contained research documents that had significant value for the company and were marked as confidential and restricted.

The next evening, Tan went to dinner with a former colleague and confessed that on a trip to China in September 2018 he had interviewed at a Chinese company and been in constant contact with company officials. The company, based in Xiamen, had developed production lines for different battery materials.

The former coworker reported the conversation to the company, which reached out to the FBI to report a theft of trade secrets. The Bureau analyzed the corporate laptop Tan had been using and found a letter from the company in Xiamen dated 15 October 2018. The letter confirmed that Tan would be the energy new material engineering center director at the company, as long as he guaranteed that information he had provided and would provide in the future was "real and effective."

Tan was charged with the theft of a trade secret, unauthorized transmission of a trade secret, and unauthorized possession of a trade secret. He later pled guilty to the charges and was sentenced to 24 months in a

U.S. federal prison for stealing information worth more than $1 billion.

"American companies invest heavily in advanced research and cutting-edge technology. Trade secret theft is detrimental to our national security and free-market economy," said Melissa Godbold, special agent in charge of the FBI Oklahoma City Field Office—which handled Tan's case. "It takes profits away from companies and jobs away from hardworking Americans. The sentencing of Hongjin Tan underscores the FBI's commitment to protecting our country's industries from adversaries who attempt to steal valuable proprietary information."

While the facts of Tan's case are unsettling, they are not entirely unusual. The FBI has more than 1,000 intellectual property (IP) theft cases open involving individuals associated with the People's Republic of China. And those thefts have cost the United States nearly $500 billion a year, says William Evanina, director of the National Counterintelligence and Security Center (NCSC).

"We've never seen the likes of economic espionage that we've seen in the past 24 months," he explains. "And a majority of that has come from the Communist Party of China."

China's Rise

Prior to the coronavirus pandemic, China's economy was growing rapidly—a trend that had continued for years, making its economy second only to that of the United States.

The expansion of China's economy followed the opening of the country in the 1980s and the growth of its middle class. The Chinese Communist Party also laid out strategic goals for the groundwork that would allow it to one day take a dominant position in producing advanced technologies to ensure its national security and global economic position.

To achieve these goals, China invested in human capital, infrastructure, and research within its own borders and abroad. It became a major investor in technology firms and promoted research and study at foreign institutions. China also weakened internal regulatory barriers for businesses—which allowed domestic firms to flourish—along with creating subsidies to build national champions.

We've never seen the likes of economic espionage that we've seen in the past 24 months.

"China's leaders want to move away from a dependence on foreign technology, so that China moves up the production value chain and is no longer just the assembler of other nations' intellectual property," wrote James Lewis, senior vice president and director of the Center for Strategic and International Studies' (CSIS) Technology Policy Program, in an analysis of China's economic and trade practices. "Since the 1980s, China has sought to build a strong technology base and has made repeated efforts to achieve this. The primary motivation is to enhance China's security and national power."

A prime example of this is China's aviation sector, which originally relied on Soviet-based manufacturers. When China opened its economy, other nations moved to partner with China to produce a better-quality product.

"Part of the requirement imposed on them for market access was coproduction, where Chinese aviation companies worked with Western aircraft firms to make parts for Western commercial aircraft or help assemble them," Lewis explained. "Coproduction, over 20 years, taught Chinese companies essential production know-how, and the quality of Chinese aircraft has improved markedly."

This improvement, in turn, might encourage the Chinese government to pressure domestic airlines to buy these Chinese-made products while also imposing barriers for foreign firms to compete in its market.

"Chinese policy is to extract technologies from Western companies; use subsidies and nontariff barriers to competition to build national champions; and then create a protected domestic market for these champions to give them an advantage as they compete globally," Lewis explained in his research. "Huawei is the best example of a globally dominant Chinese company built along these lines, but there are others. A senior Chinese official once remarked that if China had not blocked Google from the China market, there would be no Baidu," one of the largest Internet and AI companies in the world.

While much of China's ability to acquire technology and intellectual property was done through foreign direct investment, it also has carried out a broad cyber espionage campaign—beginning in the 2000s and continuing today.

"The Chinese discovered that the Internet gave them unparalleled access to poorly secured Western networks," Lewis explained. "Cyber espionage is accompanied by collection efforts by human agents, both in China and in other countries, but the most rewarding collection programs have shifted from human agents targeting Western facilities located in China to cyber espionage."

China has also engaged in a campaign of commercial espionage, targeting Western companies at an extremely high rate.

"They're not just targeting defense sector companies," said FBI Director Christopher Wray at the U.S. Department of Justice's China Initiative Conference in February 2020. "The Chinese have targeted companies producing everything from proprietary rice and corn seeds to software for wind

turbines to high-end medical devices. And they're not just targeting innovation and R&D. They're going after cost and pricing information, internal strategy documents, bulk [personally identifiable information (PII)]—anything that can give them a competitive advantage."

One example is the massive Equifax breach that compromised data on nearly every American and several thousand Canadians. Along with the charges of violating the Computer Fraud and Abuse Act, the U.S. Department of Justice also charged four members of China's People's Liberation Army (PLA) with trade secret theft for allegedly acquiring Equifax's data compilations and database designs.

"Unfortunately, the Equifax hack fits a disturbing and unacceptable pattern of state-sponsored computer intrusions and thefts by China and its citizens that have targeted personally identifiable information, trade secrets, and other confidential information," said U.S. Attorney General William Barr in a statement.

China has repeatedly denied that it was involved in any way in the Equifax breach and data theft. China's Foreign Ministry Spokesman Geng Shuang told the Associated Press that China is committed to "firmly oppose and combat cyberattacks of any kind" and that its institutions "never engage in cybertheft of trade secrets."

According to the U.S. intelligence community and the FBI, China has also targeted hospitals and research institutions to obtain insights into their work and provide it to domestic institutions. In a virtual conference hosted by the Aspen Institute in April 2020, FBI Cyber Division Deputy Assistant Director Tonya Ugoretz said the Bureau has seen increased reconnaissance and cyber intrusions of the U.S. healthcare sector and research institutions to gain insight into how they are addressing the coronavirus pandemic—especially organizations that have made announcements about their COVID-19 research.

"There are certainly good reasons for those institutions to tout the work they're doing and educate the public on the

How to Help Prevent IP Theft

To help prevent the theft of intellectual property—especially when more people than ever are working remotely and connecting to corporate assets from home—*Security Management* spoke with Sandra Stibbards, owner and president of Camelot Investigations and member of the ASIS Investigations Council.

Stibbards regularly works with clients to investigate incidents of intellectual property and trade secret theft, and to help them prevent those thefts in the future. She shared with us some of her best practices.

Check. Before a potential employee is brought on board, the organization should conduct a full background check—including full criminal and civil checks to provide information on if the individual has declared bankruptcy, has existing liens, or other judgments that the organization should be made aware of.

Stibbards also recommends employers provide notice to employees that they may do an annual update on background checks—even if the employer does not anticipate doing yearly reviews.

"It leaves them open to implementing them," Stibbards says. "All employees need to be aware that they can be looked at annually...it can keep people on the straight and narrow."

Monitor. When employees are onboarded, they should be informed that all of their activity on work computers and networks will be monitored. Employers should also set up a disclaimer that pops up every time an employee logs into their work computer to remind them.

"I advise that from day one, employees are informed that they are monitored—their work cell phone, laptop, desktop, that the company can access it at any time," she says.

Additionally, Stibbards says that IT departments should work to segment corporate networks so individuals have access only to information they need to do their job. IT should also be able to monitor that internal network to detect if an employee—or an outsider—is improperly accessing corporate data.

Educate. Employers should also educate their workforces about the threat of intellectual property and trade secret theft and how to protect themselves from falling for common attempts to obtain the ability to access that information, such as phishing attacks.

For instance, a common tactic used by malicious actors is to send an email that appears to be from a victim's bank encouraging the recipient to click a link to follow up on a reported incident of fraud.

"Don't click on anything—step outside of it. Log in directly to your bank site or call the company to verify it yourself," Stibbards says. "Take a step back, take a deep breath, and don't click or hit enter. These simple things can help avoid scams, theft of your product, or stealing of your files."

work they are doing," Ugoretz said. "The sad flip side is that it kind of makes them a mark for other nation-states that are interested in gleaning details about what exactly they're doing—and maybe even stealing proprietary information those institutions have."

This type of activity did not begin as the coronavirus was spreading, but has been occurring for some time, Evanina says, and is related to China's Thousand Talents Plan. The plan, issued in 2008, incentivizes individuals engaged in research and development in the United States to provide that knowledge to China in exchange for salaries, research funding, lab space, and more, according to a U.S. Senate Homeland Security report.

Recently, the former chair of Harvard University's Chemistry and Chemical Biology Department, Dr. Charles Lieber, was arrested and charged with making a false statement to law enforcement when he allegedly lied about being involved with the Thousand Talents Plan.

In his role at Harvard, Lieber received more than $15 million in grant funding from the National Institutes of Health and the U.S. Department of Defense for his research into nanoscience. The grant funding required him to disclose significant foreign financial conflicts of interest, such as funding from foreign governments.

"Under the terms of Lieber's three-year Thousand Talents contract, Wuhan University of Technology (WUT) paid Lieber $50,000 per month, living expenses of up to 1 million Chinese Yuan, and awarded him more than $1.5 million to establish a research lab at WUT," according to the U.S. Department of Justice (DOJ). "In return, Lieber was obligated to work for WUT 'not less than nine months a year' by 'declaring international cooperation projects, cultivating young teachers and PhD students, organizing international conference[s], applying for patents, and publishing articles in the name of' WUT."

Lieber allegedly told investigators in 2018 that he was not asked to participate in the Thousand Talents Program, but he was unable to say how China categorized his work, according to the DOJ.

> It does little good to steal intellectual property if you do not have the expertise to use it.

These kinds of partnerships, intrusions, and thefts show that while China is interested in obtaining intellectual property and trade secrets, it also needs to understand the business process to be able to use them.

"It does little good to steal intellectual property if you do not have the expertise to use it, and until recently, this was true for much of China's espionage in advanced technology," Lewis explained. "What has changed in the last decades is that China has realized that acquiring 'know-how' is more important than acquiring IP. In many cases, China now has the money and the skill to use much of the IP it has acquired licitly or illicitly."

Mitigating the Threat

While China's ability to acquire intellectual property and trade secret information is concerning for its economic impact, it also has ramifications for its adversaries' national security.

In its 2020–2022 national strategy, the NCSC included countering the exploitation of the U.S. economy as one of its strategic pillars.

"Adversaries use front companies, joint ventures, mergers and acquisitions, foreign direct investment, and talent recruitment programs to gain access to and exploit U.S. technology and intellectual property," the strategy said. "They also influence and exploit U.S. economic and fiscal policies and trade relationships."

While costing Americans billions of dollars, this transfer of knowledge "harms U.S. economic, technological, and military advantage in the world," the strategy explained. "It puts at risk U.S. innovation and the competitiveness of American companies in world markets."

And that activity is not limited to the United States alone; members of the NATO alliance are seeing similar attempts by China to acquire intellectual property and business processes, particularly in the energy sector, says Evanina, who also acts as the chair of counterintelligence for NATO.

One of the major challenges in mitigating the threat, however, was a lack of awareness from the private sector about China's activity.

"China is stealing their stuff—not our stuff," Evanina tells *Security Management*. "We need to provide information to allow CEOs to make risk-based decisions based on our strategy."

To help raise awareness, the NCSC began partnering with academic associations and U.S. Senators Richard Burr and Mark Warner to conduct briefings with college and university presidents.

"We brought in 150 university presidents and gave them a classified briefing," Evanina says. "And the FBI provided the opportunity for them to see classified cases, strategic plans by the Chinese to educate them about the threat."

The NCSC has used a similar approach to briefings with CEOs, CISOs, and CSOs. So far, Evanina estimates that they have reached 14,000 executives in the private sector where the NCSC laid out the economic impact of China's activities.

Providing this information and insight is critical, Evanina adds, because the U.S. government historically has not done the best job explaining the threat in a way that allows institutions to take action to mitigate it.

During these briefings, leaders are instructed to identify what it is their organization makes or sells that is critical to the sustainability of their company, create mechanisms to protect those assets, share the protective steps with stakeholders, and build internal employee support for protecting corporate assets.

Evanina says the briefings also focus on encouraging organizations to enhance their overall security posture and encouraging them to create insider threat programs.

"Some companies in the private sector sometimes don't want to spend a lot of money on security," he adds. "Make your security posture part of your mission. Once a quarter...we want you to bring in the following people: your CEO, general counsel, CIO, CISO, chief data officer, head of procurement, head of HR, and your head of physical security. Have a discussion about enterprisewide security... because they all need to be part of your enterprise security posture."

Evanina also suggests conducting tabletop exercises that walk stakeholders through handling a data breach or hiring an individual who turns out to be sharing trade secret information.

"Walk through that crisis plan and identify who you're going to call, how you'll notify your stockholders and shareholders and share what you've done," Evanina adds.

The NCSC's work is just one part of the executive branch's action to mitigate China's activities. The U.S. Department of Justice also stood up a China Initiative, overseen by John Demers—assistant attorney general for the National Security Division—to protect U.S. technology.

"In addition to identifying and prosecuting those engaged in trade secret theft, hacking, and economic espionage, the initiative will increase efforts to protect our critical infrastructure against external threats, including foreign direct investment, supply chain threats, and the foreign agents seeking to influence the American public and policymakers without proper registration," according to a fact sheet.

Since its inception in 2018, the China Initiative has led to numerous indictments for charges of trade secret theft and disclosure failures—like those brought against Tan and Lieber. It has also worked with companies that have had intellectual property or trade secrets stolen to prevent the thieves from turning that information into a profit.

For instance, Chinese company Fujian Jinhua allegedly stole intellectual property from U.S.-based chip manufacturer Micron. Micron coordinated with the initiative and was able to work with the U.S. federal government to file a civil lawsuit to prohibit Fujian Jinhua's ability to obtain the necessary materials to produce Micron's chips.

The U.S. Treasury Department's Committee on Foreign Investment in the United States (CFIUS) is also playing a role. The committee is required to review certain transactions that involve foreign investment in the United States—along with some real estate transactions by foreigners—to determine if they will impact America's national security.

In 2018, U.S. President Donald Trump signed into law the Foreign Investment Risk Review Modernization Act (FIRRMA). The law was designed to modernize CFIUS' role after congressional analysis by the U.S. Senate Intelligence Committee found that China was investing heavily in American technology firms to gain access to assets that could have national security ramifications.

FIRRMA allows the committee to review investment in U.S. businesses that own, operate, manufacture, supply, or serve critical infrastructure or create critical technologies. If the investment would allow a foreign government to become a partial owner, the investment could be denied on national security grounds.

"FIRRMA has been relatively successful for a number of reasons—Chinese investment has declined about three-quarters," Lewis tells *Security Management*. "Some of that was the Chinese putting restrictions on wealthy Chinese moving money out of the country, but some of it was the response to the fact that efforts to buy high-tech companies are routinely denied now."

The United States and China did sign a historic trade agreement in January 2020, which included provisions on respecting intellectual property rights and enforcement against misappropriation of trade secrets and confidential business information. But many, including Lewis, are skeptical.

"IP protection has been part of the trade deal with China, but everyone I talk to doesn't believe it will have any effect," he says. "The Chinese will agree and then continue to cheat. So, we need to think of something beyond bilateral trade deals, and the chance for partnership is out there."

Instead, Lewis says the United States will need to partner with others to prevent Chinese investment or involvement until it changes how it acquires intellectual property and shields its domestic firms from competition. In conversations with representatives from the European Union and other regions, Lewis says they also said they need to tighten their controls on Chinese investment.

"The Japanese feel that way. The Australians feel that way. The Europeans are moving in that direction, so China's behavior is causing concern for everyone," Lewis says. "That's an opportunity for the [Trump] administration. They haven't been able to take advantage of it yet, but this isn't just the United States."

Ultimately, China must be required to honor its international obligations as a member of the World Trade Organization (WTO), he adds.

"Countries that are members of WTO need to hold China accountable for its lax enforcement of IP rules," Lewis says. "I don't see that happening, but that's what it would take—for people to say this kind of behavior is unacceptable."

MEGAN GATES IS SENIOR EDITOR AT *SECURITY MANAGEMENT*. CONNECT WITH HER AT *MEGAN.GATES@ASISONLINE.ORG*. FOLLOW HER ON TWITTER: *@MGNGATES*.