ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

From Outside Assaults to Insider Threats: Chinese Economic Espionage

DARREN E. TROMBLAY | NOVEMBER 2025

China's campaign of economic espionage against the United States spans cyber intrusions, insider theft, and technology transfer disguised as collaboration. Washington must recognize that Beijing is operating an elaborate espionage ecosystem and take strategic measures to disrupt it.

KEY TAKEAWAYS

- China's espionage ecosystem is systemic and strategic. From state intelligence agencies to nominally private firms, Beijing coordinates cyber, human, and corporate channels to steal U.S. industrial and defense technologies.
- Insider threats remain the most damaging vector. Programs such as Thousand Talents and new "foreign expert" schemes have turned engineers and researchers inside U.S. firms into conduits for trade secrets.
- Chinese companies in the United States act as collection platforms. Subsidiaries and "consulting" fronts recruit American talent and channel proprietary know-how back to PRC state-owned enterprises.
- U.S. counterintelligence capacity is eroding. Shifts in FBI and DHS priorities have weakened the government's ability to detect and disrupt Chinese theft just as Beijing's efforts intensify.
- The U.S. government should respond by focusing on preemption rather on investigation. Chinese economic espionage is an ecosystem; measures can be taken to strategically disrupt it.
- While industry builds its own analytic defenses, Washington should blacklist complicit Chinese universities, tighten CFIUS oversight of greenfield investments, and integrate economic-espionage forecasting into national intelligence priorities.

CONTENTS

Key Takeaways 1
Introduction 2
Conceptual Context 3
Structures 4
Types of Compromises 5
Breaking and Entering 5
Theft by Trusted Insiders 7
Pursuing New Employment With Stolen Information 8
Opening the Door to Threat Actors 10
Persistent Penetrations 11
Going Outside 13
Outlook 18
Government Pullback 19
A Focus on Preemption 20
Endnotes 22

INTRODUCTION

The Peoples' Republic of China (PRC) has, almost since its founding, made a concerted effort to effect a shift of knowledge—and the capacity for research and development (R&D)—out of the United States. While the movement of talent is a legitimate and even beneficial aspect of innovation, the PRC has taken advantage of this dynamic to facilitate the theft of trade secrets and other proprietary information. Beijing's approach leverages the whole of society. A range of actors, including intelligence elements, companies, and students push the limits on legitimate behavior into theft.

U.S. companies are targets for multiple reasons. Historically, they have been the engines of American defense R&D, creating new capabilities such as advanced aircraft (a technology that China has historically targeted) on behalf of the government. The PRC, which has been readying for conflict, has an interest in both the technology and what it means for the United States' military posture. Even when the private sector's R&D is delinked from the U.S. government, it often focuses on areas where the PRC has been attempting to cultivate indigenous capabilities, as defined in its Made in China 2025 project.

The PRC's campaign against U.S. sources, including industry, manifests itself in multiple ways. First, Beijing is responsible for attacks from the outside against American industry as well as government and academic institutions. These often take the form of cyber intrusions, such as those conducted by Peoples' Liberation Army-affiliated hacking groups. Second, the PRC has sponsored multiple varieties of insider threats: employees who pass sensitive information to Chinese entities. Finally, PRC state-owned enterprises have used platforms in the United

States—whether local consulting firms or branches of Chinese companies—to hire human capital from U.S. industry who possess and ultimately pass trade secret information (TSI).

CONCEPTUAL CONTEXT

The PRC has consistently, explicitly advertised its intentions to engage in state-supported innovation. In 1986, the country unveiled the 863 Program, which pursued progress in supercomputing.[1] Then, in 2006, the PRC launched its Medium-to-Long Term Program for the Development of Science and Technology with the intent of facilitating indigenous innovation. Then, in 2015, the country introduced its Made in China 2025 initiative that was supposed to achieve breakthroughs in 10 high-value sectors.[2] These include next-generation information technology, robotics, aerospace, clean energy, and biotechnology.[3]

China has persistently pursued a course to acquiring identified technological expertise (as well as specific technology), as opposed to just generating it internally. This concept is entrenched and dates to the beginning of the PRC. For instance, in 1949, the Chinese in U.S. Science Association stated, as an objective, the unification and cooperation with scientific workers in the PRC to advance scientific developments in that country. In 1950, the organization received a letter from the Chinese Association of Scientific Workers asking members of the U.S. group to return to China and advised that the PRC government had established a committee to handle arrangements for this.[4]

More than 50 years later, the PRC's playbook had not substantially changed. In 2006, the Chinese government established Project 111, which had the objective of recruiting 1,000 foreign experts from the world's top 100 universities and research institutes.[5] Then, in 2008, the PRC launched its Thousand Talents Program with the intent of enticing scientists to bring their research to China. Economic espionage was a significant aspect of the Thousand Talents Program. Although many of the cases that the Department of Justice brought against talent plan participants involved academia, the private sector was not immune. In 2019, *The New York Times* reported that 600 recruits worked for U.S. companies.[6] These penetrations of the private sector, including Xiaoqing Zheng at General Electric and Xiaorong You at the Coca-Cola and Eastman Chemical, have included attempts to steal trade secrets on behalf of Chinese entities.[7]

Almost as soon as the PRC opened to the United States in 1979, the PRC looked for ways to take advantage of incoming U.S. technology.

The unmasking of the Thousand Talents Program as an inducement to espionage has forced the PRC to hide, rather than end, this way of doing business. After the U.S. began scrutinizing the Thousand Talents Program, the PRC removed a list of members from the Internet and references to the program disappeared. In place of the Thousand Talents Program, the PRC launched its National High-end Foreign Experts Recruitment Plan.[8] This new packaging of a concept that dates to the early days of the PRC targets the private sector. According to a translation of its application guide, the Recruitment Plan targets, among others, "[p]rofessional technical personnel or management personnel who hold senior positions in internationally renowned companies and institutions."[9]

Movement of expertise into the PRC's innovation ecosystem supports Chinese hard power. From its earliest decades, the PRC has attempted to identify ways to use developments in the civilian sector for military purposes. Both Mao Zedong, using the term "military-civil combination," and Deng Xiaoping pursued this transfer of knowledge.[10]

Almost as soon as the PRC opened to the United States in 1979, the PRC looked for ways to take advantage of incoming U.S. technology. For instance, journalist John Fialka has recounted how the PRC, in exchange for doing business with the McDonnell aircraft company, demanded the technology and the right to produce increasingly large pieces of the planes that it purchased in Chinese factories. As these factories absorbed the manufacturing know-how from production of nose cones and fuselages for airliners, emerging versions of Chinese fighter aircraft began featuring better-produced fuselages and aluminum skins.[11]

This process of transferring technology developed under civilian auspices to military purposes is now ingrained in the PRC's approach to innovation. In 2007, Hu Jintao made the first mention of "military-civilian fusion" (MCF).[12] In 2014, the PRC elevated MCF to a national strategy.[13] A 2020 U.S. Department of Defense report explains that MCF consists of six aspects. These include integrating and leveraging science and technology innovations across military and civilian sectors as well as cultivating talent and blending military and civilian expertise and knowledge.[14] Therefore, it can be assumed that any expertise applied on behalf of—or technology provided to—a PRC entity will support that country's ability to counter the United States and its allies militarily.

STRUCTURES

The PRC's intelligence services are key players in effecting the illicit transfer of specific technology and knowledge to that country. Civilian foreign intelligence collection is largely the domain of the Ministry of State Security (MSS). The PRC established the MSS in 1983 by merging several pre-existing entities, including several from the Ministry of Public Security (MPS)—which continues to operate. It consists of a primary central office, provincial departments, and municipal bureaus.[15] For instance, the MSS's Jiangsu Province Ministry of State Security (JSSD), has, during the past decade, been involved with the targeting of U.S. aerospace technology.[16]

Additionally, the intelligence components of the People's Liberation Army (PLA) play a significant role in the theft of U.S. private sector proprietary information. The General Staff Department Second Department (2PLA) is responsible for, among things, human intelligence (HUMINT). PRC cyber espionage against the private sector has been a persistent problem. Under the PLA, this is the responsibility of the Third Department (3PLA).[17] In 2014, the United States took the unprecedented step of indicting five Chinese hackers, working for the 3PLA's Unit 61398, in response to a campaign of trade secret theft.[18]

The PRC's private sector is complicit in the collection of intelligence. In 2015, the PRC introduced its National Security Law, which requires all parties, including the ostensible private sector to "maintain national security."[19] This was somewhat nebulous. What came next was not. The National Intelligence Law of 2017 mandated that all Chinese organizations assist with intelligence work and permitted PRC intelligence entities to establish relationships with relevant organizations.[20]

Furthermore, the PRC has demonstrated its intent to leverage the Chinese information technology sector to support cyber-facilitated intelligence activities. In 2016, the PRC instituted its Cybersecurity Law which requires telecommunications companies such as Huawei to provide the government with "technical support and assistance."[21] PRC private sector entities have repeatedly worked in conjunction with the country's intelligence services. For instance, in July 2025, the Italian government, at the request of the United States, arrested Xu Zewei, who had worked for the Shanghai Powerock Network Co. Ltd. while taking hacking direction from the MSS's Shanghai State Security Bureau.[22] Researchers at the Atlantic Council have identified the MSS's collection of vulnerabilities from private-sector partners. The researchers, Dakota Cary and Kristin Del Rosso, assessed that the MSS almost certain evaluates these for offensive use.[23]
The PRC government further co-opts business through the Chinese Communist Party (CCP). Under the 1993 Company Law, all companies that employ more than three CCP members must establish a party cell.[24] Until the ascent of Xi Jinping, the requirement was lightly enforced.[25] Since Xi's rise, the PRC government has become increasingly coercive in its use of the CCP. In 2018, new requirements mandated that publicly listed foreign joint ventures (the means by which U.S. companies do business in the PRC) establish CCP cells.[26] These cells engage in several pivotal functions including appointment of personnel and management decision-making.[27] This is apparent in the case of Cummins, a U.S.-based engine manufacturer. Cummins partnered with the PRC's Dongfeng Motor Group and, when Cummins attempted to appoint a new manager for one of its Chinese entities, the CCP vetoed the decision.[28]

The PRC has demonstrated its intent to leverage the Chinese information technology sector to support cyber-facilitated intelligence activities.

TYPES OF COMPROMISES

Chinese actors have used a variety of methods to exfiltrate private sector data. These have ranged from simple theft (especially cyber attacks), to insider threats (individuals courted by Chinese entities walking out the door with sensitive information), to sophisticated, longer-term operations directed at reaching into companies to co-opt individuals with access—and willingness to transfer—proprietary information.

Breaking and Entering

The PRC has long-established itself as a practitioner of cyber espionage. While the technology employed in this is distinctly 21st century, there is nothing particularly novel about the underlying concept: simple theft by breaking and entering.

Multiple hacking efforts by PRC entities had targeted the U.S. government in the first decade of the 21st century. The threat for industry, however, became stunningly apparent in 2010, when Google announced that China had stolen portions of the company's source code in an attack referred to as Operation Aurora. This hack also targeted several dozen other corporations ranging from Intel to Morgan Stanley.[29]

Operation Aurora emanated from Chinese academic institutions. According to *The New York Times*, investigators linked the hackers to Shanghai Jiaotong University, which, at the time, had one of the PRC's leading computer science programs. Other participants, the Times reported,

appeared to be affiliated with the Lanxiang Vocational School, which trains computer scientists for the PRC military.[30]

It is unlikely happenstance that these attacks emanated from academic institutions. As *The Economist* noted in 2025, the Chinese Communist Party (CCP) has a long history of shaping students' educational decisions.[31] A profusion of malicious computer science students is consistent with the PRC's agenda. China's use of academic institutions as cover for intelligence activity has become a routine practice in both the cyber and HUMINT domains.

While Operation Aurora was the first significant warning that the PRC was turning its cyber resources on the private sector, it was not the first instance of this. Following Google's announcement, researchers at the cybersecurity firm McAfee identified a cyberespionage campaign, which they named Night Dragon, that had been targeting multiple U.S. oil companies—specifically for business data such as bid information and potential sites for future operations—since 2008.[32] According to *The Christian Science Monitor*, which broke the story, the PRC's exact role in Night Dragon was unknown, but information flowing from at least one company's computer was going back to China.[33]

Night Dragon's targeting is consistent with subsequent PRC attacks. In 2018, for instance, the U.S. indicted two PRC MSS-affiliated hackers who, between 2006 and 2018, targeted a wide variety of companies, from across multiple industries, including one involved in oil and gas drilling, production, and processing.[34]

Identifying that these threat activities were ongoing was the first step toward curbing the PRC cyberthreat. In 2014, the United States, for the first time, indicted five Chinese military hackers on economic espionage and related charges. These individuals were officers in the PLA Third Department's Unit 61398. Targets included Westinghouse technology, SolarWorld business information (including attorney-client communications regarding litigation about Chinese solar product manufacturers' "dumping" practices), and Alcoa internal discussions about a partnership with a PRC state-owned enterprise.[35]

PRC entities have employed increasingly sophisticated ruses to facilitate social engineering ploys such as phishing emails.

The 2014 indictment set for the stage for what can only be described as a naive agreement on the U.S. government's part. In 2015, President Barack Obama announced that he had reached an agreement with the PRC's Xi Jinping that "neither the U.S. or the Chinese government will conduct or knowingly support cyber-enabled theft of intellectual property … for commercial advantage."[36]

It was unlikely that a practitioner of outright theft, such as the PRC, would uphold its end of the bargain. The cybersecurity firm FireEye initially tallied that network compromises by PRC-backed hacking groups had dropped from 60 in early 2013 to fewer than 10 by mid-2016. As the Council on Foreign Relations' Adam Segal cautioned, however, "Absence of evidence is not the same thing as evidence of absence, and the Chinese may be becoming more stealthy and sophisticated in their attacks."[37]

PRC state-sponsored hacking continued, as indicated by subsequent indictments. In 2021, the U.S. charged personnel associated with the MSS's Hainan State Security Department (HSSD) with an extensive hacking campaign, between 2011 and 2018.[38] Targets included a U.S. information technology company located in California; a U.S. defense contractor, also located in that state; a U.S. company in the mid-Atlantic region involved with the manufacture of aircraft and marine craft; an aircraft servicing company headquartered in New Jersey with repair and maintenance services at airports globally; a U.S. airline; and a U.S. defense contractor headquartered in Virginia, which was involved with maritime R&D.[39]

This case showed the continuing relationship between Chinese intelligence and higher education. Members of the HSSD-led conspiracy worked with staff and professors at both an identified PRC university and college to identify and recruit talented computer hackers. Additionally, members of the conspiracy worked with those institutions to identify and recruit linguists capable of interpreting stolen material.[40]

These attacks did not require an insider threat but, when necessary, exploited mistakes by targeted companies' employees. Spear-phishing emails got Chinese actors into company systems. In 2009, a Google employee received a message with an embedded link, which they clicked and opened the door to Operation Aurora.[41] (In early 2010, *Reuters* reported that Google was also looking at whether individuals working in Google China's office facilitated the attack.[42]) A similar ruse, using an email that appeared to be sent by a Marathon Oil employee, containing a link, introduced the Night Dragon attack.[43]

PRC entities have employed increasingly sophisticated ruses to facilitate social engineering ploys such as phishing emails. For instance, in the 2021 case, involving the HSSD, conspirators employed doppelganger domain names, which intentionally resembled links to legitimate companies. This increased the chances that a harried employee, skimming the email, would take the bait. Additionally, conspirators created fictitious online profiles, associated with spear-phishing email accounts, to increase the appearance of legitimacy.[44]

Outsider attacks may also use very traditional, physical means. For instance, in 2004, an employee of the Chinese telecom firm Huawei entered a trade show in the middle of the night, after the event had concluded and visited the booth of a technology company. The employee's badge listed his employer as "Weihua" ("Huawei" with the syllables reversed). Once at the booth, the employee removed the cover from a networking device and took photographs of the circuitry inside.[45]

Theft by Trusted Insiders

The PRC has not simply smashed and grabbed with cyberattacks. It has benefitted from the perfidy of trusted insiders who have helped Beijing to siphon off proprietary information. Programs such as Thousand Talents and its successors have encouraged the illicit transfer of knowledge as individuals, whether for patriotism or profit, have crossed the line from the legitimate pursuit of opportunities to engage in theft.

Insider threats take three primary forms. The simplest takes the form of employees who end their employment by walking out of their employers' doors with privileged information. More complex are those individuals who remain employed by the private sector but, throughout this

employment, transfer information to Chinese entities. The third form of insider threat is those employees who unlock doors for other PRC actors.

Pursuing New Employment With Stolen Information

Over approximately the past decade, the U.S. government has disrupted multiple efforts by individuals to transfer information from their private sector employers to entities in the PRC. A number of these instances have occurred under the auspices of the Thousand Talents Program. Although the program has a new name, it is unlikely, given the trajectory of China's approach to illicit technology transfer, that the basic concept will change.

The case of Yu Long provides an example of how the PRC has attempted to penetrate the defense sector. In 2013, Long expressed interest in and was subsequently accepted to the Thousand Talents Program.[46] The PRC asked Long to provide documents, to validate claims in his TTP application, acquired through his work at the United Technologies Research Center (which included work with companies including Pratt & Whitney and Sikorsky).[47] Long explicitly stated that his aim was to "help China to mature its own aircraft engines."[48] In November 2014, Long was arrested after trying to fly to the PRC with export-controlled and proprietary documents related to F-22 and F-35 engines.[49] Long eventually pleaded guilty to conspiracy to steal trade secrets knowing that this would benefit a foreign government, foreign instrumentality, or foreign agent.[50]

Xiaorong You is another individual who envisioned profiting from her employers by leveraging TSI to obtain a payment from the Thousand Talents (as well as a local version of the) program. The TSI at stake was bisphenol-A (BPA)-free coating for food packaging. (BPA, which had been used to minimize flavor loss and prevent containers from corroding or reacting with their contents, was linked to possible harmful effects, hence the need for an alternative.)[51]

The Coca-Cola Company employed You as the principal engineer for global research between 2012 and 2017.[52] In this capacity, You had access to TSI belonging to six companies including Dow Chemical and Sherwin Williams.[53] While still employed by Coca-Cola, You agreed with Liu Xiangchen, and co-conspirator #1, to transfer stolen TSI to the Chinese company Weihai Jinhong Group and become an employee of that company. Xiangchen would arrange for the Chinese company to not only pay You for her participation in the conspiracy but also assist her in obtaining Thousand Talent and locally distributed provincial government awards.[54]

You lied to one employer and penetrated another for the purpose of stealing TSI. When she left Coca-Cola in August 2017, she signed a written agreement, falsely attesting that she had not retained and no longer had access to TSI or other confidential information. The same month You agreed to this, she opened files on a computer containing TSI and took photographs of the screen to bypass security measures. In September 2017, she obtained employment at Eastman Chemical Company in part to steal TSI information in furtherance of the conspiracy. She took photographs of Eastman's laboratory equipment, located in secure and restricted locations, to show Xiangchen the industrial equipment needed. Upon learning that Eastman planned to fire her, You uploaded company TSI to her Google drive.[55]

The conspiracy had the potential to significantly damage U.S. R&D. Companies involved in developing BPA-free coatings had spent approximately $120 million to develop it.[56] You and her Chinese corporate partner Weihai Jinhong Group received millions of dollars in Chinese grants to

support a second company, owned in part by Weihai Jinhong Group, You, Liu, and co-conspirator #1. This second company would partner with an Italian company for the purpose of establishing a market presence in China for the TSI that You had furnished to Weihai Jinhong Group. The conspirators planned to compete with U.S. companies, including some of the owners of the stolen TSI, in China and globally.[57]

Fortunately, for the companies involved, the U.S. government identified and disrupted You's conspiracy. In April 2021, a federal jury convicted You of multiple crimes including conspiracy to commit trade secret theft, conspiracy to commit economic espionage, and economic espionage.[58]

The PRC academic apparatus—students and institutions—have facilitated penetration of U.S. entities by insider threats. Wei Pang came to the United States in 2001 as a Ph.D. candidate at the University of Southern California (USC). Almost immediately after graduating in 2006, Pang took a job with Avago, which produced bulk acoustic wave (BAW) filters for wireless devices. Avago's technology contained trade secrets. Another Chinese student, Hao Zhang, also earned a Ph.D. at USC and, after graduating in 2006, took a job with Skyworks, an innovator of semiconductors. Huisui Zhang earned a masters degree in electrical engineering, in 2006 from USC as well, and went to work for Micrel Semiconductor.[59]

The PRC academic apparatus—students and institutions—have facilitated penetration of U.S. entities by insider threats.

Shortly after entering the U.S. technology sector, all three individuals began to develop a plan for exfiltrating trade secrets from Avago and Skyworks. Their plan was to establish a BAW fabrication facility in the PRC—an objective that they explicitly linked to improving PRC military capabilities. In 2006, Huisui Zhang emailed Wei Pang and Hao Zhang notes about establishing a BAW fabrication facility in the PRC (the understanding that this would involve illicit activity was confirmed shortly thereafter by a warning from Pang to maintain secrecy about the plan). Pang later suggested that they call the company "cliftbaw" for "China lift BAW technology."[60]

A Chinese university became a conspirator in this plan. Tianjin University (TJU) was a member institution of the PRC's 985 Project—which provided state funding to develop flagship schools.[61] TJU entered into a joint venture with Wei Pang, Hao Zhang, and others as a vehicle to "launder" trade secrets for use by TJU in establishing its own fabrication facility. The university even provided guidance for establishing a shell company in the Cayman Islands that would appear to the be source for the trade secrets stolen from Avago and Skyworks.[62]

To establish academic legitimacy that would justify their hiring by TJU, Pang and Hao Zhang needed patents. Both individuals applied for patents using technology and trade secrets they stole from their respective employers. Hao Zhang applied for the U.S. patents in order to keep Avago's name off the information that was coming from it through Pang. The corresponding PRC patents were filed under both Pang's and Hao Zhang's names.[63] The U.S. victims only learned of their loss when Pang's former boss traveled to Tianjin to visit Pang and recognized the stolen Avago technology in Pang's laboratory.[64]

One by one, the conspirators departed the United States for the safety of the PRC. Hao Zhang left Skyworks on June 9, 2009 (he had previously suggested to a TJU official that he remain in the U.S. long enough to "master the technology" he was working on at Skyworks).[65] On June 29, 2009, Wei Pang departed Avago and relocated to the PRC.[66] The United States, however, arrested Hao Zhang when, on May 16, 2015, he re-entered the United States.[67] In 2020, Zhang was convicted on charges including economic espionage and theft of trade secrets and ordered to pay nearly half a million dollars in restitution.[68]

Opening the Door to Threat Actors

Insider threats have not only acquired information themselves, they have also made it easier for other PRC threat actors to obtain it. As *The Economist* noted in 2024, the Chinese Academy of Sciences has filed 192 patents for seeds.[69] Approximately 10 years before this story was filed, Weiqiang Zhang, a Chinese citizen who was in the United States where he had earned his Ph.D. as a legal permanent resident and was employed as a rice breeder for Ventria Bioscience, which produced genetically programmed rice used in therapeutic and medical fields, wrote from his work email, "I try hard to promote scholarly interchange of technology between [the Crops Research Institute in Tianjin, China] researchers and American scholars as well as the scientists from American biotech companies so that we can learn from their advanced technology and use it for our benefit."[70] Zhang continued that Ventria "is the only biotech company in the U.S. that has the ability to produce and sell recombinant protein products from growing rice seeds. I hope in the near future, Tianjin, China will have the same capability."[71]

Zhang's letter does not appear to have been idle musing. In 2013, Zhang had helped to coordinate the travel of a PRC crop research delegation to the United States. When the delegation prepared to depart, a Customs and Border Protection (CBP) search of its luggage found numerous seeds in envelopes labeled with words or initials that correlated with their contents. An expert rice geneticist employed by the U.S. Department of Agriculture recognized some of these markings as indicating Ventria products. When the FBI subsequently searched Zhang's home, it discovered two types of seeds in his freezer that were only produced by Ventria and that matched seeds found on the delegation returning to the PRC.[72] In 2017, Zhang was convicted of one count of conspiracy to steal trade secrets (the seeds were patented but the research and protocols used for making them cost-effectively were considered a trade secret), one count of conspiracy to commit interstate transportation of stolen property, and one count of interstate transportation of stolen property.[73]

Agricultural espionage by the PRC has yielded indications of an insider threat that has yet to be resolved. Mo Hailong, a PRC national who became a legal U.S. permanent resident via an H-1B visa, was the director of International Business for the Beijing Dabeinong Technology Group Company (which had a subsidiary, King's Nower Seed, responsible for corn seed). Hailong approached the grower of a Pioneer Hi-Bred Corporation test field in Iowa in May 2011 and wanted to know what he was planting. Accompanying Hailong was Wang Lei, the vice chairman of King's Nower Seed. After learning that the grower was planting corn seed, Hailong returned the following day and began digging in the field before the field manager confronted him. Several months later, Hailong, Lei, and Li Shaoming (a Ph.D. scientist and CEO at Kings Nower Seed) were found at another field in Iowa, which was growing bio-engineered corn seed for Monsanto. Hailong's activities, according to the FBI, suggested that there were "several potential 'insiders' at U.S. based seed companies" who were providing Hailong with locations of test fields being

used for growing bio-engineered seed.[74] Although these insiders were not identified, Hailong pled guilty in 2016 to charges of conspiring to steal trade secrets from DuPont (the parent company of Pioneer) and Monsanto.[75]

The PRC has also employed insiders with access to targeted companies in furtherance of sophisticated cyberintrusion campaigns. In 2017, a U.S. grand jury indicted participants in a JSSD for a sophisticated attack targeting turbofan engine technology being developed through a partnership between a French firm and a U.S. aerospace company. In 2013, a JSSD intelligence officer (IO) met with Tian Xi, an employee of the French firm, who worked in the firm's Suzhou, China, office as a product manager.[76] The JSSD provided Xi with malware, which Xi used to infect the firm's computers using a USB drive.[77] Additionally, the JSSD co-opted the firm's Information Technology Infrastructure and security manager at the Suzhou office, who provided the JSSD with information about the firm's internal investigation of the JSSD computer intrusions.[78]

Agricultural espionage by the PRC has yielded indications of an insider threat that has yet to be resolved.

This JSSD hacking campaign also clearly illustrates how Chinese state hackers could turn companies' IT infrastructure against themselves. In 2010, members of the conspiracy infiltrated the network of Capstone Turbine—a U.S.-based gas turbine manufacturer—and created an email account on the server (thereby appearing to be legitimate, from within the company) and used it for spear phishing. A member of the conspiracy also installed malware onto Capstone Turbine's web server to facilitate a "watering hole" attack. This type of attack involves the installation of malware onto legitimate web pages to facilitate intrusions of computers that visit those pages.[79]

Persistent Penetrations

Several Chinese economic espionage cases have involved the persistent penetrations of U.S. companies, rather than individuals' illegally facilitated changes in career, which are uniquely damaging. They provide opportunities for PRC entities to remain current on developments within U.S. industry rather than simply acquire increasingly stale stolen material.

The Dongfan "Greg" Chung case was a particularly pernicious penetration. Chung was an employee of Rockwell (and later Boeing after it acquired Rockwell) between 1973 and 2002. As early as 1979, Chung volunteered his services to Chen Lung Ku at the PRC's Harbin Institute of Technology, explaining that Chung had been "a Chinese compatriot for over thirty years" and was "proud of the achievements by the people's efforts for the motherland."[80] Chung expressed his regret that he had not contributed anything so far and volunteered his services. It did not take long for Chen to reply, stating, "We'd like to join our hands together with the overseas compatriots in the endeavor for the construction of our great socialist motherland."[81] This desire to "join our hands together" echoed the relationship between the Chinese in the U.S. Science Association and the Chinese Association of Scientific Workers.

Multiple PRC aerospace entities began soliciting assistance from Chung. In 1985, the China National Aero Technology Import and Export Corporation made suggestions for topics that Chung should cover when delivering lectures in the PRC.[82] (Chung provided lectures in the PRC between 1985 and 2003.[83]) Then, the PRC's Nan Chang Aircraft Company contacted Chung,

who subsequently advised the company that he had started collecting manuals from the Rockwell subsidiary North American Aviation. The PRC clearly viewed Chung as a versatile asset. A third entity, the China Aviation Industry Corporation, contacted Chung in 1987 to ask for technical assistance with several issues, including development of a "space shuttle orbiter."[84]

It was clear that Chung knew he was working for a foreign government. For instance, in 1985, he passed manuals to the Nan Chang Aircraft Company via the Education Consul at the PRC's San Francisco, California, consulate.[85]

Chung was also clearly aware that he was engaged in a clandestine relationship. When a representative of PRC's Ministry of Aviation and the China Aviation Industry Corporation was making arrangements for one of Chung's visits to the PRC, the representative suggested "cover stories" that Chung could use to explain his travel.[86] When Chung learned that he was going to be laid off from Boeing, he began to surreptitiously dispose of documents he had collected from the company, hiding them between pages of newspapers, which he recycled.[87] When the FBI searched Chung's house in 2006, it discovered more than 250,000, pages of documents from Rockwell, Boeing, and other defense contractors both within the house and secreted in a crawl space underneath it.[88]

In 2009, a three-week bench trial found Chung guilty of offenses including six counts of economic espionage.[89] Chung's case was a landmark in the United States' campaign against the illicit acquisition of corporate information and was the first time that there had been a trial conviction under the 1996 Economic Espionage Act.

The PRC's Ministry of State Security has had a direct role in seeking recruitments in the private sector.

Chung, however, would hardly be the last Chinese insider threat engaged in espionage against the U.S. private sector. In 2008, General Electric (GE) hired Xiaoqing Zheng, a dual U.S. and Chinese citizen, as a principal engineer to work on turbine sealing technology. While he was still in the employ of GE, Zheng was selected in 2012 for the PRC's Thousand Talents program. This should have been a warning sign. Then, in 2014, GE corporate security learned that Zheng had copied 19,020 electronic files from one of his GE-issued computers onto a thumb drive. Zheng's next step, like his Thousand Talents participation, further suggested that he was trying to bridge two worlds, to GE's detriment. In 2015, he established the Nanjing Tainyi Aeronautical Technology Ltd. in Nanjing, China. Despite potential conflicts of interest, GE did not tell Zheng that his involvement with the company—a parts supplier for civil aviation engines—was unacceptable. (Subsequently reviewing public Internet sites, GE realized that Zheng was working on the same types of technology for PRC entities that he was for GE.) Zheng, in 2018, used steganography (concealing a data file within another data file) to hide files on his GE computer before emailing them to his personal account.[90]

Zheng's dual life finally came to an end when, in March 2022, a jury trial convicted him of conspiracy to commit economic espionage. Trial evidence showed that Zheng and others in the PRC had conspired to steal GE trade secrets pertaining to ground-based and aviation-based turbine technologies, with the intent to benefit PRC-based companies and universities that research, develop, and manufacture turbine parts.[91]

The PRC's MSS has had a direct role in seeking recruitments in the private sector. Yanjun Xu was a deputy division director in the MSS who was responsible for obtaining trade secrets from aviation and aerospace companies in the United States. The Nanjing University of Aeronautics and Astronautics (NUAA) worked with Xu to target an engineer at GE Aviation.[92] Reaching out via LinkedIn, an NUAA official invited the engineer to deliver a research presentation.[93] Xu's NUAA coconspirator gave the GE Aviation engineer very specific parameters for the presentation, asking him to focus on highly technical topics including the latest developments in the application of GE Aviation's signature material used in aeroengines, as well as engine structure design analysis technology and manufacturing technology development. The PRC had used a similar methodology with Chung. Although the email was signed by an NUAA official, it came from one of Xu's email accounts.[94]

The presentation allowed Xu to surface and take over the relationship from NUAA. An NUAA official made the introduction between Xu and the engineer, wherein Xu presented himself as being affiliated with the Jiangsu Science and Technology Association. During the first few months of 2018, Xu and the engineer corresponded with Xu raising the possibility of the engineer returning to NUAA; in January 2018, he advised the engineer that he was consulting with the department to identify which technology was of interest. Shortly thereafter, Xu broached the idea of meeting with the engineer during a business trip to Europe. In preparation for this, Xu asked the engineer to export a GE Aviation file directory onto a hard drive. Xu's expectation that he would be running an ongoing penetration of GE Aviation was apparent in his suggestion that this meeting would not be the last one, since they would be doing business together.[95] It was, however, the last one. When Xu arrived in Belgium, expecting to receive information from his GE Aviation source, authorities arrested him and extradited him to the United States, where he became the first MSS officer to stand trial in a U.S. courtroom.[96]

Going Outside

The PRC, in addition to recruiting insider threats, has used U.S.-based platforms to hire expertise from which it then siphons trade secrets and other protected information. These platforms include businesses formed in the United States that serve as intermediaries for recruiting specific talents. They also take the form of PRC subsidiaries that have established a presence within the United States.

China's pursuit of the ability to produce titanium dioxide (TiO_2) via a chloride route eventually used a U.S.-based consulting firm to acquire trade secrets. TiO_2 is a white pigment used in a wide variety of products ranging from paints to food (it is, among other things, what gives Oreo filling its color). E. I. du Pont de Nemours & Company (DuPont) invented the chloride route process—which consists of multiple trade secrets—to manufacture TiO_2 in the 1940s.[97]

The PRC was intent on acquiring chloride route TiO_2 technology, having publicly identified it as a scientific and economic priority.[98] In the early 1990s, the Chinese government attempted to purchase TiO_2 technology from DuPont in furtherance of building its own plant. DuPont was charging $75 million to license its technology and the PRC opted, for the time being, to pursue a TiO_2 production method developed in the former Soviet Union. Starting in 2000, DuPont began exploring the possibility of building its own TiO_2 plant in China and, by 2007, it had obtained some of the government approvals for the project. By 2008, however, the project had stalled

because DuPont could no longer get information about the project's status from government officials.[99]

What DuPont did not know was that the PRC had not been deterred by DuPont's uninterest. In 1991, Walter Liew attended a banquet hosted by high-level PRC officials who identified him as "a patriotic overseas Chinese" who had provided the PRC with "key technologies."[100] At this banquet, the secretary general of China's State Council gave Liew "directives" about future contributions he could make to the PRC. Liew subsequently received a list of "key task[s]" that identified chloride route TiO_2 production as one of the "more important projects."[101]

Liew was a businessman. In the 1990s, he and his wife founded USA Performance Technology Inc (UAPTI), a provider of engineering consulting services.[102] Liew, in 1997, met two former DuPont employees, Robert Maegerle and Tim Spitler, a project engineer and chemical engineer, respectively, who had experience with TiO_2 facilities. When these individuals retired from DuPont, they agreed "not to use or divulge … any secret or confidential information" without DuPont's permission.[103] By early 1998, Liew had assembled a team of former DuPont employees, under USAPTI's direction. It did not take long for this team to begin passing proprietary information. In March 1998, Maegerle sent a fax to Liew that contained DuPont TSI as well as information about plant costs and personnel data, the latter of which would be useful to a company trying to develop facilities to compete with DuPont. Maegerle continued to provide Liew and USAPTI with DuPont trade secrets into 2010.[104]

The PRC government was still interested in acquiring TiO2 chloride route technology. China's State-Owned Assets Supervision and Administration Commission of the State Council (SASAC) controlled the Pangang Group Company Limited. When Liew learned that one of Pangang's subsidiaries planned to build a 30,000 metric tons per year (MTPY) TiO2 chloride process plant, he wrote letters, advising that he possessed the complete TiO_2 process technology and attempted to sell his services to Pangang. In 2005, Liew signed a $6.2 million with one of Pangang's subsidiaries to develop a 30,000 metric-ton-per-year TiO_2 project. He followed this up in 2009 by signing a $17.8 million contract with another Pangang subsidiary for a 100,000 metric-ton-per-year TiO_2 project. In August 2009, USAPTI delivered design information to Pangang that contained numerous features based on technology directly misappropriated from DuPont.[105]

Pursuit of TiO_2 shows that the use of U.S. platforms to gather proprietary information was not limited to Liew's dealings with Pangang. Tze Chao had been a DuPont employee between 1966 and 2002 before becoming a consultant to the Pangang Group in 2003. Chao bid against USAPTI for the 2009 contract that the latter won.[106] In the course of the ultimately unsuccessful negotiations, the Pangang Group agreed that it would work with Chao's firm Cierra if it employed former DuPont employees and possessed blueprints for DuPont's TiO_2 plants.[107] It is worth noting that a Pangang Group official asked Chao to review the work that USAPTI had provided, in 2009, approximately a month after USAPTI provided it.[108] Chao provided a report to Pangang, with recommendations for improving USAPTI's designs; these recommendations drew on DuPont's trade secrets.[109]

Liew's prosecution was a landmark in economic espionage law. It was the first time a federal jury had convicted on charges brought under the Economic Espionage Act of 1996.[110] In 2014, Liew received a 15-year sentence and was ordered to forfeit $278 million in illegal profits and pay

$511,687.82 in restitution for what the judge described as a "white collar crime spree."[111] Chao had already pled guilty in 2012 to conspiracy to commit economic espionage.[112]

The PRC used a similar approach to acquire nuclear technology. Szuhsiung Ho was the owner and president of Delaware-based Energy Technology International (ETI) and served as a senior advisor to the China Guangdong Nuclear Power Company (CGNPC). The CGNPC is a state-owned enterprise controlled by SASAC, with a board of directors composed of Communist Party of China members.[113] (SASAC also controlled Pangang, which had used a similar playbook to acquire chloride route TiO_2 technology.)

Ho and ETI engaged in talent acquisition on behalf of CGNPC. Ho, in October 2009, indicated that "China has the budget to spend. They asked me if I could form a comprehensive team to provide technology transfer in design and manufacturing, related training, and technical supports."[114] According to Ho, CGNPC wanted to "bypass the research stage and go directly to the final design and manufacturing phase."[115]

It was apparent that Ho was targeting expertise in a specific U.S. company. In December 2009, he recruited multiple U.S. persons (USPERs) to assist CGNPC with its fuel design program. In his pitch, he indicated that he was interested in retired or active employees from a specific U.S. company, but cautioned, "Please help but do not openly announce this news. I don't want to alert [the U.S. company]."[116] Ho made a similar pitch in early 2012, when he sought assistance in recruiting small modular reactor experts and asked an individual to "spread the words to your [U.S. company] colleagues (current or retired colleagues) but without revealing CGNPC intention to build such reactors."[117]

It was apparent that the U.S. company was at risk of losing information. In April 2012, Ho recruited a third USPER from the company who later advised that the USPER would be able to give CGNPC useful information that was not in the normal company presentations.[118]

Ho's actions were not economic espionage per se, but were a similar movement of restricted information from the U.S. private sector to a PRC government-controlled entity. In 2016, a federal grand jury indicted Ho on a charge of conspiring to engage or participate in the development or production of special nuclear material in China without specific authorization to do so from the U.S. secretary of Energy.[119] The grand jury also indicted Ho on a charge of acting as a foreign agent.[120] Ho pled guilty to the special nuclear material charge and was sentenced to 24 months in prison.[121] Had he been convicted of the foreign agent charge, he would have faced a potential life sentence.[122]

A variation on the theme of U.S. companies funneling talent illicitly to the PRC is the employment of USPERs by U.S. elements of Chinese technology firms. For instance, Baidu—a Chinese firm that has become heavily involved with artificial intelligence (AI)—has sought to tap Silicon Valley expertise by establishing its first office there in 2011 and following that up in 2017 by establishing an R&D center.[123] Baidu's announcement of its R&D center illustrates how China can tap into U.S. talent to support innovation by companies ultimately beholden to Beijing. In 2014, the company announced that the center was to be led by an individual who had previously helmed Stanford University's AI lab and had also helped Google establish its own AI efforts.[124] It is a short step for an individual once hired by a Chinese firm to furnish trade

secrets, whether intentionally or simply by incorporation of knowledge into work product, from a previous employers.

The PRC has taken an aggressive position in the South China Sea. Consistent with this, it has sought to develop marine engineering equipment that could survive at significant depths. This led the PRC to identify the need for a material called syntactic foam. In furtherance of conducting research on this material, PRC government entities, including three state-owned enterprises, partnered with the Taizhou CBM Future New Material Science and Technology Co. Ltd. (CBMF) in China's Zhejiang Province. CBMF planned to sell syntactic foam to the PRC military and state owned enterprises.[125]

Acquisition of syntactic foam technology bore resemblances to the Walter Liew and Szuhsiung Ho cases. The difference is that the U.S.-based entity siphoning local talent was directly controlled by the PRC. Shan Shi became president of CBM International (CBMI), which was established in Houston, Texas, during 2014. CBMF was the only shareholder in CBMI and Shan Shi was, in turn, a shareholder of CBMF who had been involved with the design of at least one PLA Navy ship.[126] Shi had pledged to build "China's first deep[-]sea drilling buoyance [*sic*] material production line" based on what he could "digest / absorb" from the United States.[127]

Business arrangements that span the United States and the PRC have been conduits for the siphoning of autonomous vehicle technology.

CBMI hired, directly and indirectly, individuals who had worked for the Swedish company Trelleborg Offshore, with a subsidiary in Houston, Texas, that focused on development of syntactic foam. Samuel Ogoe had been employed by the Swedish company before going to work for CBMI. In 2015, Ogoe was in contact with multiple employees of Trelleborg Offshore who provided Ogoe with three trade secrets. Information about at least one of these secrets went from Ogoe to another CBMI employee to CBMF. Shi used another firm, Offshore Drilling Inc. (ODI), which he owned, as a cover for recruiting additional expertise. Greg Liu was a Chinese citizen who had arrived in the United States on a student visa. (This status brings to mind the origins of the threats to Avago and Skyworks.) Eventually, Liu obtained employment with Trelleborg Offshore as a material development engineer. After Liu was laid off from that job, Shi offered Liu full-time employment at ODI to conceal the work that Liu would be doing for CBMI from Trelleborg Offshore. Liu provided CBMI and CBMF personnel with four additional trade secrets while employed by ODI. In June 2016, Shi dropped the charade and transferred Liu to CBMI.[128]

In 2019, Shi was convicted on one count of conspiracy to commit theft of trade secrets.[129] He received a 16-month prison sentence and was ordered to forfeit more than $330,000.[130]

Business arrangements that span the United States and the PRC have been conduits for the siphoning of autonomous vehicle technology. In 2015, TuSimple, a self-driving-truck developer, began operations in 2015, in California.[131] The company was founded by two Chinese entrepreneurs and backed by a Chinese media mogul. (In the authoritarian PRC, it is difficult to believe that media strays too far from the government's line.) TuSimple developed technology in the United States. This problem was similar to that presented by Baidu's and Huawei's leveraging of U.S. talent. Some of this technology was developed in conjunction with American companies such as Navistar.[132]

TuSimple was intertwined with PRC-based entities. After establishing TuSimple, one of its co-founders established a PRC-located startup in 2021 called Hydron—which develops hydrogen-powered trucks—backed by the same mogul who had backed TuSimple.[133] Hydron recruited TuSimple employees, with some continuing to work for the former company.[134] The two companies shared an office in Beijing. TuSimple employees working in the Beijing office routinely downloaded autonomy source code, via joint access to a repository, developed by U.S.-based engineers.[135]

These ostensibly private companies had links to the PRC government. In 2021, Hydron, which was informed by TuSimple's technology, reached a deal to develop autonomous trucks with Foton, a Chinese company. Foton was a subsidiary of Beijing Automotive Group Co., Ltd. (BAIC), a PRC state-owned company. BAIC had an agreement with a Chinese military university that was doing work on driverless technology.[136]

Subsidiaries of Chinese companies operating in the United States can facilitate the illicit transfer of knowledge through employment. In 2018, for instance, Xiaolang Zhang, who was hired by Apple to work on an autonomous vehicle project, downloaded trade secret intellectual property shortly before departing the company to take a position with Xiaopeng Motors, a Chinese electric vehicle company, which had offices in Palo Alto, California. According to Zhang, he planned to work for the Chinese competitor on the same technologies that he had developed for Apple.[137] Zhang, in 2022, pled guilty to one count of theft of trade secrets.[138] It is worth noting that Zhang's case was one of three Chinese cases that targeted Apple's autonomous car project.[139]

The PRC's massive telecommunications company, Huawei, has capitalized on its U.S. presence.

Another one of the Apple penetrations highlights the threat that companies such as Baidu pose. In 2016, Apple hired Weibao Wang as a software engineer. Wang worked on the Apple team that designed and developed hardware and software that had applications for self-driving cars. In late 2017, Wang accepted an offer of full-time employment as a staff engineer with the U.S.-based subsidiary of a PRC company that was working on self-driving car technology. Wang waited for more than four months before advising Apple that he had accepted a new position. This gap could give Wang time to learn what his new employer wanted to know from Apple. In the days leading up to his departure from Apple, in April 2018, Wang accessed large amounts of sensitive proprietary and confidential information.[140] Wang then fled the United States for Guangzhou, China.[141] Once in the PRC, he became an executive at a joint venture between Baidu and Chinese automaker Geely.[142] If Baidu was willing to employ an individual accused of trade secret theft in the PRC, what was it doing much closer to U.S. tech firms in Silicon Valley?

The PRC's massive telecommunications company, Huawei, has capitalized on its U.S. presence. It has a facility in Plano, Texas, and an R&D center in Northern California.[143] The company has weaponized recruitment against U.S. firms. Shortly after the founding of one U.S. company (referred to in a 2020 indictment as "Company 6"), which was poised to compete directly against Huawei in the field of memory hardware architectural design, Huawei launched an initiative to continuously recruit employees of Company 6 to cause "internal turmoil" at its competitor.[144]

Even more perniciously, Huawei has functioned as a de facto intelligence service. In 2013, it launched a bonus program to reward employees who obtained confidential information from competitors. There was a formal rewards schedule to pay employees of Huawei affiliates based on the value of information they obtained. Employees who acquired information of interest were supposed to post it to an internal Huawei website or, if it was particularly sensitive, send it via encrypted email to a special "huawei.com" email inbox.[145]

Huawei's activities in the field of joint ventures show how the PRC has subverted business norms to achieve an unfair advantage vis-à-vis U.S. competitors. In 2009, the Huawei subsidiary Futurewei targeted a technology company (referred to in a USG indictment as "Company 4") for technology related to antennas that provide cellular telephone and data services. Futurewei approached this through the guise of a joint venture. In September 2009, Futurewei entered into a non-disclosure agreement (NDA) with Company 4, which was supposed to prevent Futurewei from using any of Company 4's confidential information to Futurewei's benefit or to the competitive disadvantage of Company 4. Futurewei received TSI from Company 4 in late September 2009. It took Futurewei only approximately a month to file a provisional patent application with the U.S. Patent and Trademark Office that relied in large part on Company 4's intellectual property.[146]

Chinese economic espionage and economic espionage-adjacent cases at least partially debunk a widely repeated generalization about PRC spying. Paul Moore, who intelligence historian David Wise characterized as the FBI's "former senior China analyst," for instance, characterized Chinese intelligence collection as consisting of numerous individuals, each collecting small amounts of information, equivalent to tourists picking up grains of sand on a beach, rather than targeting specific items.[147] Another former FBI official, I.C. Smith, testified to the U.S. China Economic and Security Commission that "there is, often times, little specific targeting of information or technology by the Chinese."[148]

The PRC, however, has engaged in what appears to be targeted collection against several technologies, consistent with the objectives it has articulated. Multi-person targeting of specific technologies (e.g., the 2018 thefts of Apple autonomous vehicle technology—consistent with the Made in China 2025 objective of developing high-end computerized machines) suggests that collection is coordinated. Relatedly, the case of CBMI indicates that collection is not opportunistic. The PRC identified a technology it wanted (again consistent with a Made in China 2025 objective—new materials) and developed a specific intelligence operation to obtain it.

Furthermore, the PRC has taken a multi-vector approach to obtain information on specific topics: PRC actors attacked U.S. turbine technology through both human and technical penetrations. The JSSD compromised the network of Capstone Turbine. Several years later, Zheng Xiaoqing engaged in theft from GE.

OUTLOOK

The private sector needs to maintain a robust analytic capability to ferret out threats and address vulnerabilities. While cybersecurity is the hottest topic, it is the lowest hanging fruit. Companies need to start with geopolitical analysis of the PRC's objectives and assess how China may seek to enhance its capabilities through espionage. It then needs to identify its own vulnerabilities to human, as well as technical, penetrations and take steps to harden these areas. This should be

informed by maintaining an ongoing awareness of the methodologies and tactics PRC actors use, such as the establishment of U.S. firms that siphon expertise that is then transmitted to Chinese state-affiliated entities.

Industry can benefit from partnering with the government, but it should also be maintaining or acquiring its own intelligence capabilities. Government has historically proven to be a valuable partner in developing counterintelligence awareness, and the private sector's position as the first target of economic espionage means that it is uniquely positioned to be a good corporate citizen by providing authorities with its observations. Government priorities, however, do change as the United States deals with what it deems to be the most pressing national security issues.

Government Pullback

The FBI, for instance, has historically, on multiple occasions, shifted resources away from counterintelligence. In 1992, under the mistaken impression that the Cold War had conclusively ended, the Bureau reassigned approximately 300 agents from counterintelligence to investigating violent crime.[149] This reassessment led to the creation of the Safe Streets Task Forces. More recently, as at the end of the Cold War in 1991, the FBI—consistent with the White House's prioritization—has identified the need to "crush violent crime" as an objective.[150] Consistent with this, in August 2025, the FBI's Washington Field Office reassigned agents from areas including counterintelligence to work against local criminal activities in Washington, D.C.[151] Addressing illegal migration has also led to a reprioritization of resources. In October 2025, *The Washington Post* reported, based on data obtained by Sen. Mark Warner (D-VA), that the Bureau had reassigned approximately 25 percent of its total agents to immigration enforcement (with the largest field offices dedicating more than 40 percent of their allotment to this challenge).[152] Some of these agents were drawn from the fields of counterintelligence and cybercrime.[153] While it is the administration's prerogative to assess threats and how best to address them, counterintelligence, particularly combating economic espionage and trade secret theft, is an essential mission that should be maintained and adequately resourced.

A desire to do more with less may also diminish the U.S. government's ability to assist the private sector. For instance, the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) lost approximately 1,000 employees to buyouts and layoffs during the first few months of the second Trump administration.[154] A significant CISA function, often in collaboration with the FBI, is warning the private sector about network vulnerabilities. Such awareness helps to get in front of PRC cyberactors before they can exploit information technology systems to pilfer private sector secrets.

Another DHS component, Homeland Security Investigations (HSI) plays a sometimes-overlooked role in combating Chinese theft against the U.S. private sector. For instance, between 2011 and 2013, Wenxia Man conspired to illegally export multiple fighter jet engines and an MQ-9 drone to China.[155] (The aerospace sector is one of the 10 identified in the Made in China 2025 plan.[156]) It was an undercover HSI agent who learned, from Man, that her coconspirator Xinsheng Zhang, located in the PRC, was a "technology spy" who worked on behalf of the Chinese military to copy purloined items.[157] The second Trump administration, according to the Cato Institute, has opted to reorient HSI agents from their investigatory activities to focus on immigration enforcement.[158]

Cuts to government spending may impose a "brain drain" on the private sector. Technology companies' R&D has historically received support from the U.S. government, so reductions in spending may lead firms to downsize and lay off human capital. China continues to pursue cutting-edge technology that has been developed in the private sector. For instance, in 2023, a Google employee working on AI applied to a Chinese talent program and founded his own company in the PRC.[159] The United States is already seeing China attempting to recruit former U.S. government scientists with opportunities for career development.[160] If the private sector follows suit and downsizes due to a reduction in government spending, China may employ similar techniques against laid off personnel.

A Focus on Preemption

Limited resources mean that the U.S. government should focus on preemption rather than investigation. Chinese economic espionage is an ecosystem, and measures can be taken to strategically disrupt it.

The porousness between Chinese academic institutions and the PRC government has proven to be an ongoing problem. The United States in 2025 announced that it would start revoking visas of Chinese students with connections to the Chinese Communist Party or studying in critical fields.[161] This should be supplemented. Multiple cases have highlighted specific Chinese schools whose students have been linked to the theft of trade secrets and proprietary information. **The United States should blacklist these Chinese institutions and reject their students' visa applications**.

China is using the United States' capacity for innovation against it. PRC companies including tech heavyweights Baidu and Huawei have engaged in R&D in the United States. The presence of such firms amounts to helping Beijing innovate against Washington. Currently, despite the Foreign Investment Risk Review Modernization Act of 2018, the Committee on Foreign Investment in the United States (CFIUS) is still not able to block certain types of greenfield investments (i.e., nonacquisition) that would empower a foreign adversary such as China. At the same time, both Chinese firms and government venture funds invest in U.S. technology company startups and are usually able to avoid CFIUS scrutiny. **New CFIUS legislation should set parameters—and impose meaningful oversight—on the type of activities that Chinese companies operating within the United States can engage in.**

The U.S. Intelligence Community is essential to identifying foreign developments that will inform economic espionage. For instance, determining Chinese geopolitical objectives will help the United States to understand what capabilities it needs and what it will likely target. The President's Intelligence Priorities (PIP), conveyed through the National Intelligence Priorities Framework (NIPF), inform "resource allocations to ensure collection and analysis of intelligence that provides insights, warning or other illuminating information on the priorities."[162] The NIPF in turn translates and implements national intelligence priorities "to ensure the IC is focusing its collection, analysis, and operational resources on the most urgent and important national security issues."[163]

Topics that help the United States forecast trends in economic espionage and trade secret theft by the PRC should be incorporated into the PIP and cascading NIPF if they are not already included. Multiple topics can help the U.S. government to disrupt economic espionage and trade secret theft before these manifest themselves in specific crimes that harm the private sector. Collection should include Chinese innovation strategies such as the Made in China 2025 plan; geopolitical

objectives including a focus on the South China Sea that new capabilities such as syntactic foam might support; relationships with third countries through which China might already be obtaining technology; China's intelligence services' methodologies and tactics; and security vulnerabilities in U.S. industry's business practice. Analysis should turn this data into an awareness of how these variables might interplay to create risks and, from there, provide recommendations for solutions.

Ultimately, the PRC-U.S. contest over technology secrets is not trench warfare, but rather a continually evolving fight. PRC objectives will continue to change, as their geopolitical objectives shift, and this will inform its targeting of specific industries, companies, and technologies. Changes in how the countries interact—both in the human and technical spaces—will shape intelligence methodologies and tradecraft. The U.S. government's ability to disrupt economic espionage—especially through preemptive, strategic measures—will mitigate risk to industry. Finally, U.S. industry's investment in its own protection—analysis of geopolitics cascading into ramifications for intelligence that informs countermeasures—will be essential to the protection of its assets.

About the Author

Darren Tromblay served as an intelligence analyst and applied historian in the U.S. Intelligence Community for more than two decades. He has authored multiple books on aspects of national security, including *Spying: Assessing U.S. Domestic Intelligence Since 9/11*, *The FBI Abroad: Bridging the Gap between Domestic and Foreign Intelligence*, and *Securing the Private Sector: Protecting U.S. Industry in Pursuit of National Security*. His work has also been featured in multiple peer-reviewed journals including *The International Journal of Intelligence and Counterintelligence* and *Intelligence and National Security*. Tromblay holds an M.A. from the Elliott School at George Washington University, an M.S. from the National Intelligence University, and a B.A. from the University of California at Riverside.

About ITIF

The Information Technology and Innovation Foundation (ITIF) is an independent 501(c)(3) nonprofit, nonpartisan research and educational institute that has been recognized repeatedly as the world's leading think tank for science and technology policy. Its mission is to formulate, evaluate, and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress. For more information, visit itif.org/about.

ENDNOTES

1. Hearing on Made in China 2025—Who Is Winning?, "Before the U.S. China Economic and Security Review Commission," February 6, 2025, https://www.uscc.gov/sites/default/files/2025-02/February_6_2025_Hearing_Transcript.pdf.
2. U.S.-China Economic and Security Review Commission, "2024 Report to Congress, Chapter 3,U.S. China Competition in Emerging Technologies."
3. John C. Demers, Assistant Attorney General, National Security Division, Department of Justice, Statement for the Record for the Senate Committee on the Judiciary, "China's Non-Traditional Espionage Against the United States: The Threat and Potential Policy Responses." December 12, 2018 https://nsarchive.gwu.edu/media/17990/ocr.
4. Federal Bureau of Investigation. Potentialities of Chinese Communist Intelligence Activities in the United States. 1954.
5. Sean O'Connor, "How Chinese Companies Facilitate Technology Transfer from the United States" (Washington, D.C.: U.S.—China Economic and Security Review Commission. 2019), https://www.uscc.gov/sites/default/files/Research/How%20Chinese%20Companies%20Facilitate%20Tech%20Transfer%20from%20the%20US.pdf.
6. Ellen Barry and Gina Kolata. "China's Lavish Funds Lured U.S. Scientists. What Did It Get in Return?" *The New York Times*, February 6, 2020, https://www.nytimes.com/2020/02/06/us/chinas-lavish-funds-lured-us-scientists-what-did-it-get-in-return.html.
7. U.S. Attorney's Office. Eastern District of Tennessee. "Ph.D. Chemist Convicted of Conspiracy to Commit Economic Espionage, Theft of Trade Secrets, and Wire Fraud," April 22, 2021, https://www.justice.gov/usao-edtn/pr/phd-chemist-convicted-conspiracy-commit-economic-espionage-theft-trade-secrets-and-wire; United States Attorney's Office, Northern District of New York. "Former GE Power Engineer Sentenced for Conspiracy to Commit Economic Espionage," January 3, 2023, https://www.justice.gov/usao-ndny/pr/former-ge-power-engineer-sentenced-conspiracy-commit-economic-espionage.
8. Barry and Kolata. "China's Lavish Funds Lured U.S. Scientists. What Did It Get in Return?"
9. 2020 National Foreign Expert Project Application Guide, https://cset.georgetown.edu/publication/2020-national-foreign-expert-project-application-guide/.
10. "Commercialized Militarization: China's Military—Civil Fusion Strategy," National Bureau of Asian Research, June 30, 2021, https://www.nbr.org/publication/commercialized-militarization-chinas-military-civil-fusion-strategy/; Elsa B. Kania and Lorand Laskai, "Myths and Realities of China's Military-Civil Fusion Strategy" (Washington, D.C.: Center for a New American Security. 2021), https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/Myths-and-Realities-of-China's-Military-Civil-Fusion-Strategy_FINAL-min.pdf; Emily de la Bruyere and Nathan Picarsic, "Defusing Military-Civil Fusion: The Need to Identify and Respond to Chinese Military Companies" (Washington, D.C.: Foundation for Defense of Democracies. 2021), https://www.fdd.org/wp-content/uploads/2021/05/fdd-monograph-defusing-military-civil-fusion.pdf.
11. John J. Fialka, *War by Other Means: Economic Espionage in America* (New York: Norton, 1999).
12. Audrey Fritz, "China's Evolving Conception of Civil Military Collaboration," Center for Strategic & International Studies, August 2, 2019, https://www.csis.org/blogs/trustee-china-hand/chinas-evolving-conception-civil-military-collaboration.
13. "Commercialized Militarization: China's Military—Civil Fusion Strategy," National Bureau of Asian Research, June 30, 2021, https://www.nbr.org/publication/commercialized-militarization-chinas-military-civil-fusion-strategy/.

14. Department of Defense, "Military and Security Developments Involving the People's Republic of China 2020," https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF.
15. China's Intelligence Services and Espionage Operations, "Hearing Before the U.S.—China Economic and Security Review Commission," June 09, 2016 https://www.uscc.gov/sites/default/files/transcripts/June%2009%2C%202016%20Hearing%20Transcript.pdf.
16. U.S. Department of Justice, "Year in Review for China-Related Cases," December 5, 2018, https://www.justice.gov/usdoj-media/opa/media/983321/dl?inline; https://www.justice.gov/d9/press-releases/attachments/2018/10/30/indictment_zhang_et_al_0.pdf; U.S. Department of Justice, "Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years," October 30, 2018, https://www.justice.gov/archives/opa/pr/chinese-intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal.
17. China's Intelligence Services and Espionage Operations, "Before the U.S.-China Economic and Security Review Commission," June 09, 2016, https://www.uscc.gov/sites/default/files/transcripts/June%2009%2C%202016%20Hearing%20Transcript.pdf.
18. U.S. Department of Justice, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," May 19, 2014, https://www.justice.gov/archives/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.
19. Feng, "We Can't Tell if Chinese Firms Work for the Party: Huawei claims to be an independent firm, but China's own laws mandate a different reality," Foreign Policy, February 7, 2019, https://foreignpolicy.com/2019/02/07/we-cant-tell-if-chinese-firms-work-for-the-party/.
20. National Intelligence Law. https://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf.
21. Ashley Feng, "We Can't Tell if Chinese Firms Work for the Party: Huawei claims to be an independent firm, but China's own laws mandate a different reality," Foreign Policy February 7, 2019, https://foreignpolicy.com/2019/02/07/we-cant-tell-if-chinese-firms-work-for-the-party/.
22. U.S. Department of Justice, "Justice Department Announces Arrest of Prolific Chinese State-Sponsored Contract Hacker," July 8, 2025, https://www.justice.gov/opa/pr/justice-department-announces-arrest-prolific-chinese-state-sponsored-contract-hacker.
23. Dakota Cary and Kristin Del Rosso. "Sleight of hand: How China weaponizes software vulnerabilities," The Atlantic Council, 2023, https://www.atlanticcouncil.org/in-depth-research-reports/report/sleight-of-hand-how-china-weaponizes-software-vulnerability/.
24. Lin Yang and Liam Scott, "Chinese Subsidiary of British Investment Bank Now Includes Communist Party Committee," Voice of America, August 03, 2022, https://www.voanews.com/amp/chinese-subsidiary-of-british-investment-bank-now-includes-communist-party-committee/6684911.html; Rush Doshi, "China's New National Security Laws: Risks to American Companies and Conflicts of Interest," Before the U.S. Senate Committee on Homeland Security and Governmental Affairs, Hearing on "Safeguarding the Homeland: Examining Conflicts of Interest in Federal Contracting to Protect America's Future," September 24, 2024, https://cdn.cfr.org/sites/default/files/report_pdf/Testimony-Doshi-2024-09-24.pdf.
25. Yang and Scott, "Chinese Subsidiary of British Investment Bank Now Includes Communist Party Committee," Voice of America, August 03, 2022, https://www.voanews.com/amp/chinese-subsidiary-of-british-investment-bank-now-includes-communist-party-committee/6684911.html.

26. Doshi, "China's New National Security Laws: Risks to American Companies and Conflicts of Interest."
27. U.S. China Economic and Security Review Commission, 2021 Report to Congress, 2021, https://www.uscc.gov/sites/default/files/2021-11/Chapter_2_Section_3--Chinese_Governments_Evolving_Control_of_the_Nonstate_Sector.pdf.
28. Alexandra Stevenson. "China's Communists Rewrite the Rules for Foreign Businesses," *The New York Times*, April 13, 2018, https://www.nytimes.com/2018/04/13/business/china-communist-party-foreign-businesses.html.
29. Michael Joseph Gross, "Enter the Cyber-dragon," *Vanity Fair*, September 2011, https://www.vanityfair.com/news/2011/09/chinese-hacking-201109?srsltid=AfmBOorJ1h7mnjK4wq5D24_k2KMrYori3HvqFICW5-CIrnSIo4sY6eZ7.
30. John Markoff and David Barboza, "2 China Schools Said to Be Tied to Online Attacks," *The New York Times*, February 18, 2010, https://www.nytimes.com/2010/02/19/technology/19china.html.
31. "China's New Army of Engineers," *The Economist*, June 26, 2025.
32. Bobbie Johnson, "Oil companies targeted by hacking attack," *The Guardian*, January 27, 2010, https://www.theguardian.com/technology/2010/jan/27/oil-hacking.
33. Mark Clayton, "U.S. oil industry hit by cyberattacks: Was China Involved?" *The Christian Science Monitor*, January 25, 2010, https://www.csmonitor.com/USA/2010/0125/US-oil-industry-hit-by-cyberattacks-Was-China-involved.
34. U.S. Department of Justice, "Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information," December 20, 2018, https://www.justice.gov/archives/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.
35. U.S. Department of Justice, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," May 19, 2014, https://www.justice.gov/archives/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.
36. Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference, September 25, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint.
37. Adam Segal, "The U.S.—China Cyber Espionage Deal One Year Later," Council on Foreign Relations, September 28, 2016, https://www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later.
38. U.S. Department of Justice, "Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information Including Infectious Disease Research," July 19, 2021, https://www.justice.gov/archives/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion.
39. *United States of America v. Ding Xiaoyang; Cheng Qingmin; Zhu Yunmun; and Wu Shurong*.
40. Ibid.
41. Kim Zetter, "Google Hack Attack Was Ultra Sophisticated, New Details Show," *Wired*, January 14, 2010, https://www.wired.com/2010/01/operation-aurora/.
42. "Google probing possible inside help on attack," *Reuters*, January 19, 2010, https://www.reuters.com/article/technology/google-probing-possible-inside-help-on-attack-idUSTRE60H1J6/.
43. Clayton, "U.S. oil industry hit by cyberattacks: Was China involved?"

44. *United States of America v. Ding Xiaoyang; Cheng Qingmin; Zhu Yunmun; and Wu Shurong*.
45. *UNITED STATES OF AMERICA—against—HUAWEI TECHNOLOGIES CO., LTD., HUAWEI DEVICE CO., LTD., HUAWEI DEVICE USA INC., FUTUREWEI TECHNOLOGIES, INC., SKYCOM TECH CO., LTD., WANZHOU MENG*, also known as "Cathy Meng" and "Sabrina Meng," https://www.justice.gov/archives/opa/press-release/file/1248961/dl?inline=.
46. Deborah Kidwell, "A case of economic espionage," Office of Special Investigations, September 24, 2020, https://www.osi.af.mil/News/Features/Display/Article/2359612/a-case-of-economic-espionage/.
47. "Man charged with trying to take U.S. military documents to China," *Reuters*, December 9, 2014, https://www.reuters.com/article/world/man-charged-with-trying-to-take-u-s-military-documents-to-china-idUSKBN0JN2LI/.
48. Deborah Kidwell, "A case of economic espionage," Office of Special Investigations, September 24, 2020, https://www.osi.af.mil/News/Features/Display/Article/2359612/a-case-of-economic-espionage/; Federal Bureau of Investigation, "Former Connecticut Resident Charged with Attempting to Travel to China with Stolen U.S. Military Program Documents," December 9, 2014, https://www.fbi.gov/contact-us/field-offices/newhaven/news/press-releases/former-connecticut-resident-charged-with-attempting-to-travel-to-china-with-stolen-u.s.-military-program-documents.
49. Ibid.
50. Ibid.
51. *United States of America v. Xiaorong You (aka Shannon You and Liu Xiangchen).*
52. Ibid.; United States Attorney's Office, Eastern District of Tennessee, "PH.D. Chemist Sentenced to 168 Months for Conspiracy to Steal Traded Secrets, Economic Espionage, Theft of Trade Secrets, and Wire Fraud," May 9, 2022, https://www.justice.gov/usao-edtn/pr/phd-chemist-sentenced-168-months-conspiracy-steal-traded-secrets-economic-espionage.
53. Ibid.
54. *United States of America v. Xiaorong You (aka Shannon You and Liu Xiangchen).*
55. Ibid.
56. United States Attorney's Office, "PH.D. Chemist Sentenced to 168 Months for Conspiracy to Steal Traded Secrets, Economic Espionage, Theft of Trade Secrets, and Wire Fraud."
57. *United States of America v. Xiaorong You (aka Shannon You and Liu Xiangchen).*
58. United States Attorney's Office, "PH.D. Chemist Sentenced to 168 Months for Conspiracy to Steal Traded Secrets, Economic Espionage, Theft of Trade Secrets, and Wire Fraud."
59. *United States of America v. Wei Pang, Hao Zhang, Huisui Zhang, Jinping Chen, Zhao Gang, and Chong Zhou.*
60. Ibid.
61. U.S.-China Economic and Security Review Commission, "2023 Report to Congress," 2023, https://www.uscc.gov/sites/default/files/2023-11/Chapter_3_Section_1--China_Educating_and_Training_Its_Next_Generation_Workforce.pdf.
62. *United States of America v. Wei Pang, Hao Zhang, Huisui Zhang, Jinping Chen, Zhao Gang, and Chong Zhou.*
63. Ibid.
64. Ellen Nakashima, "Grand Jury Indicts Six Chinese Citizens in Alleged Plot to Steal Trade Secrets," *The Washington Post*, May 20, 2015.
65. *United States of America v. Wei Pang, Hao Zhang, Huisui Zhang, Jinping Chen, Zhao Gang, and Chong Zhou.*

66. Ibid.
67. U.S. Department of Justice, "Chinese Professors Among Six Defendants Charged with Economic Espionage and Theft of Trade Secrets for Benefit of People's Republic of China," May 19, 2015, https://www.justice.gov/archives/opa/pr/chinese-professors-among-six-defendants-charged-economic-espionage-and-theft-trade-secrets.
68. United States Attorney's Office, Northern District of California, "Chinese Citizen Sentenced for Economic Espionage, Theft of Trade Secrets, and Conspiracy," September 1, 2020, https://www.justice.gov/usao-ndca/pr/chinese-citizen-sentenced-economic-espionage-theft-trade-secrets-and-conspiracy.
69. "China has become a scientific superpower," *The Economist*, June 12, 2024, https://www.economist.com/science-and-technology/2024/06/12/china-has-become-a-scientific-superpower.
70. *United States vs. Weiqiang Zhang and Wengui Yan*, https://www.courtlistener.com/docket/5243268/1/united-states-v-zhang/.
71. *Ibid*
72. Ibid.
73. U.S. Department of Justice, "Chinese Scientist Sentenced to Prison in Theft of Engineered Rice," April 4, 2018, https://www.justice.gov/archives/opa/pr/chinese-scientist-sentenced-prison-theft-engineered-rice; *United States vs. Weiqiang Zhang and Wengui Yan*.
74. *United States of America v. Mo Hailong also known as Robert Mo*.
75. U.S. Department of Justice, "Chinese National Pleads Guilty to Conspiring to Steal Trade Secrets," January 27, 2016, https://www.justice.gov/archives/opa/pr/chinese-national-pleads-guilty-conspiring-steal-trade-secrets.
76. *United States of America v. Zhang Zhang-Gui; Zha Rong; Chai Meng; Liu Chunliang; Gao Hong Kun; Zhuang Xiaowei; Ma Zhiqi; Li Xiao; Gu Gen; and Tian Xi*.
77. U.S. Department of Justice, "Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years," October 30, 2018, https://www.justice.gov/archives/opa/pr/chinese-intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal.
78. *United States of America v. Zhang Zhang-Gui; Zha Rong; Chai Meng; Liu Chunliang; Gao Hong Kun; Zhuang Xiaowei; Ma Zhiqi; Li Xiao; Gu Gen; and Tian Xi.*
79. Ibid.
80. *United States of America v. Dongfan 'Greg' Chung*, https://caselaw.findlaw.com/court/us-9th-circuit/1581047.html.
81. *Ibid.*
82. Ibid.
83. Federal Bureau of Investigation, "Former Boeing Engineer Sentenced to Nearly 16 Years in Prison for Stealing Aerospace Secrets for China," February 08, 2010, https://archives.fbi.gov/archives/losangeles/press-releases/2010/la020810.htm.
84. *United States of America v Dongfan 'Greg' Chung*.
85. Ibid.
86. Ibid.
87. Ibid.

88. Federal Bureau of Investigation, Former Boeing Engineer Sentenced to Nearly 16 Years in Prison for Stealing Aerospace Secrets for China."
89. U.S. Department of Justice, Former Boeing Engineer Convicted of Economic Espionage in Theft of Space Shuttle Secrets for China."
90. *United States of America v Xiaoqing Zheng*.
91. Ibid.
92. *United States of America vs. Yanjun Xu.*
93. Yudhijit Bhattarcharjee, "The Daring Ruse That Exposed China's Campaign to Steal American Secrets," *The New York Times*, March 7, 2023, https://www.nytimes.com/2023/03/07/magazine/china-spying-intellectual-property.html.
94. *United States of America vs. Yanjun Xu.*
95. Ibid.
96. United States Attorney's Office. Southern District of Ohio. "Chinese government intelligence officer sentenced to 20 years in prison for espionage crimes, attempting to steal trade secrets from Cincinnati company," November 16, 2022, https://www.justice.gov/usao-sdoh/pr/chinese-government-intelligence-officer-sentenced-20-years-prison-espionage-crimes.
97. *United States of America v. Walter Lian-Heen Liew; Christina Hong Qiao Liew; Robert J. Maegerle; USA Performance Technology Inc; Tze Chao, Hou Sendone; Pangang Group Company Ltd., Pangang Group Steel Vanadium & Titanium Company Ltd, Pangang Group Titanium Industry Company Ltd. and Pangang Group International Economic & Trading Company. [Superseding Indictment].*
98. Ibid.
99. *United States of America v Walter Liew; United States of America v USA Performance Technology Inc.*
100. Ibid.
101. Ibid.
102. "US man sentenced for selling DuPont secrets to China," BBC, July 11, 2014, https://www.bbc.com/news/world-asia-china-28258454; *United States of America v. Walter Lian-Heen Liew; Christina Hong Qiao Liew; Robert J. Maegerle; USA Performance Technology Inc; Tze Chao, Hou Sendone; Pangang Group Company Ltd., Pangang Group Steel Vanadium & Titanium Company Ltd, Pangang Group Titanium Industry Company Ltd. and Pangang Group International Economic & Trading Company. [Superseding Indictment].*
103. *United States of America v Walter Liew; United States of America v USA Performance Technology Inc.*
104. *United States of America v. Walter Lian-Heen Liew; Christina Hong Qiao Liew; Robert J. Maegerle; USA Performance Technology Inc; Tze Chao, Hou Sendone; Pangang Group Company Ltd., Pangang Group Steel Vanadium & Titanium Company Ltd, Pangang Group Titanium Inustry Company Ltd. and Pangang Group International Economic & Trading Company. [Superseding Indictment].*
105. Ibid.
106. Federal Bureau of Investigation, "Former DuPont Scientist Pleads Guilty to Economic Espionage," March 02, 2012, https://archives.fbi.gov/archives/sanfrancisco/press-releases/2012/former-dupont-scientist-pleads-guilty-to-economic-espionage.
107. *United States of America v. Walter Lian-Heen Liew; Christina Hong Qiao Liew; Robert J. Maegerle; USA Performance Technology Inc; Tze Chao, Hou Sendone; Pangang Group Company Ltd., Pangang Group Steel Vanadium & Titanium Company Ltd, Pangang Group Titanium Industry Company Ltd. and Pangang Group International Economic & Trading Company. [Superseding Indictment].*

108. Ibid.
109. Ibid.
110. Federal Bureau of Investigation, "Two Individuals and Company Found Guilty in Conspiracy to Sell Trade Secrets to Chinese Companies," March 05, 2014, https://archives.fbi.gov/archives/sanfrancisco/press-releases/2014/two-individuals-and-company-found-guilty-in-conspiracy-to-sell-trade-secrets-to-chinese-companies.
111. United States Attorney's Office, Northern District of California, "Walter Liew Sentenced to Fifteen Years in Prison for Economic Espionage," July 11, 2014, https://www.justice.gov/usao-ndca/pr/walter-liew-sentenced-fifteen-years-prison-economic-espionage.
112. Federal Bureau of Investigation, "Former DuPont Scientist Pleads Guilty to Economic Espionage."
113. *United States of America v Szuhsiung Ho a/k/a Allen Ho, China General Nuclear Power Company a/k/a China Guangdong Nuclear Power Company and Energy Technology Int.*
114. Ibid.
115. Ibid.
116. Ibid.
117. Ibid.
118. Ibid.
119. U.S. Department of Justice, "U.S. Nuclear Engineer Pleads Guilty to Violating the Atomic Energy Act," January 6, 2017, https://www.justice.gov/archives/opa/pr/us-nuclear-engineer-pleads-guilty-violating-atomic-energy-act.
120. Ellen Nakashima and Steven Mufson, "U.S. Used Cold War-era statute to prosecute Taiwanese American nuclear engineer," *The Washington Post*, January 6, 2017, https://www.washingtonpost.com/world/national-security/us-used-cold-war-era-statute-to-prosecute-chinese-american-nuclear-engineer/2017/01/06/6842e878-c6c2-11e6-bf4b-2c064d32a4bf_story.html.
121. U.S. Department of Justice, "U.S. Nuclear Engineer Sentenced to 24 Months in Prison for Violating the Atomic Energy Act," August 31, 2017, https://www.justice.gov/archives/opa/pr/us-nuclear-engineer-sentenced-24-months-prison-violating-atomic-energy-act; U.S. Department of Justice. U.S. Nuclear Engineer Pleads Guilty to Violating the Atomic Energy Act."
122. Nakashima and Mufson. "U.S. Used Cold War-era statute to prosecute Taiwanese American nuclear engineer."
123. Sherisse Pham. "Why China still needs Silicon Valley," CNN, December 16, 2018, https://www.cnn.com/2018/12/16/tech/china-tech-silicon-valley.
124. Paul Mazar and Rolfe Winkler, "Baidu to Open Artificial Intelligence Center in Silicon Valley," *The Wall Street Journal*, May 16, 2014, https://www.wsj.com/articles/SB10001424052702304908304579565950123054242.
125. *United States of America v Shan Shi; Kui Bo; Gang Liu; Sam Ogoe; Uka Uche; Huang Hui; and Johnny Wade Randall.*
126. Ibid.
127. United States Attorney's Office, District of Columbia, "American Businessman Who Ran Houston-Based Subsidiary of Chinese Company Sentenced to Prison for Theft of Trade Secrets," February 11, 2020, https://www.justice.gov/usao-dc/pr/american-businessman-who-ran-houston-based-subsidiary-chinese-company-sentenced-prison.
128. *United States of America v Shan Shi; Kui Bo; Gang Liu; Sam Ogoe; Uka Uche; Huang Hui; and Johnny Wade Randall.*

129. U.S. Department of Justice, "Texas Man Convicted of Conspiracy to Commit Theft of Trade Secrets. July 29, 2019," https://www.justice.gov/archives/opa/pr/texas-man-convicted-conspiracy-commit-theft-trade-secrets.
130. U.S. Department of Justice, "American Businessman Who Ran Houston-Based Subsidiary of Chinese Company Sentenced to Prison for Theft of Trade Secrets."
131. Heather Somerville, Kate O'Keefe, and Yang Jie. "TuSimple Probed by FBI, SEC Over Its Ties to a Chinese Startup," *The Wall Street Journal*, October 30, 2022, https://www.wsj.com/articles/tusimple-probed-by-fbi-sec-over-its-ties-to-a-chinese-startup-11667159325.
132. Heather Somerville, "The Self-Driving Truck Startup That Siphoned Trade Secrets to Chinese Companies," *The Wall Street Journal*, May 27, 2025, https://www.wsj.com/tech/china-self-driving-trucks-tusimple-c20255e1.
133. Ibid.
134. Somerville, O'Keefe, and Jie, "TuSimple Probed by FBI, SEC Over Its Ties to a Chinese Startup."
135. Somerville. "The Self-Driving Truck Startup That Siphoned Trade Secrets to Chinese Companies."
136. Ibid.
137. *United States of America v. Xiaolang Zhang.*
138. United States Attorney's Office, Northern District of California, "Former Apple Employee Indicted on Theft of Trade Secrets," July 16, 2018, https://www.justice.gov/usao-ndca/pr/former-apple-employee-indicted-theft-trade-secrets; Kif Leswing, "Former Apple engineer accused of stealing automotive trade secrets pleads guilty," CNBC, August 22, 2022, https://www.cnbc.com/2022/08/22/former-apple-employee-xiaolang-zhang-pleads-guilty-.html.
139. Rohan Goswami and Kif Leswing, "Ex-Apple employee accused of stealing trade secrets is exec at Baidu self-driving car joint venture," CNBC, May 16, 2023, https://www.cnbc.com/2023/05/16/ex-apple-employee-accused-of-stealing-secrets-is-jidu-automotive-exec.html; Lauren Feiner, "A second Apple self-driving car engineer is accused of stealing trade secrets," CNBC, January 30, 2019, https://www.cnbc.com/2019/01/30/apple-autonomous-vehicle-engineer-accused-of-stealing-trade-secrets.html; Rohan Goswami, "DOJ charges former Apple engineer with theft of autonomous car tech for China," CNBC, May 16, 2023, https://www.cnbc.com/2023/05/16/doj-charges-former-apple-engineer-with-theft-of-autonomous-car-tech-for-china.html.
140. United States Attorney's Office, Northern District of California. Former Apple Employee Charged With Theft of Trade Secrets," May 16, 2023, https://www.justice.gov/usao-ndca/pr/former-apple-employee-charged-theft-trade-secrets.
141. *United States of America v. Weibao Wang*, https://fm.cnbc.com/applications/cnbc.com/resources/editorialfiles/2023/05/16/apple-engineer-indictment.pdf.
142. Goswami and Leswing "Ex-Apple employee accused of stealing trade secrets is exec at Baidu self-driving car joint venture."
143. Rhodium Group, "New Neighbors 2018 Update: Chinese Investment in the United States by Congressional District," 2018, https://rhg.com/research/new-neighbors-2018/.
144. *UNITED STATES OF AMERICA against HUAWEI TECHNOLOGIES CO., LTD., HUAWEI DEVICE CO., LTD., HUAWEI DEVICE USA INC., FUTUREWEI TECHNOLOGIES, INC., SKYCOM TECH CO., LTD., WANZHOU MENG, also known as "Cathy Meng" and "Sabrina Meng,"* https://www.justice.gov/archives/opa/press-release/file/1248961/dl?inline=
145. Ibid.
146. Ibid.

147. David Wise, *Tiger Trap: America's Secret Spy War with China* (Boston: Houghton Mifflin Hartcourt, 2011).
148. China's Propaganda and Influence Operations, Its Intelligence Activities that Target the United States, and the Resulting Impacts on U.S. National Security, Before the U.S. China Economic and Security Review Commission, 111th Cong. (2009).
149. Sharon LaFraniere. "FBI Reassigning 300 Counterspies to Crime-Fighting," *The Washington Post*, January 9, 1992, https://www.washingtonpost.com/archive/politics/1992/01/09/fbi-reassigning-300-counterspies-to-crime-fighting/5dd51ad5-1148-4360-a363-bd562127b6d0/.
150. Department of Justice, Justice Operations, Management, and Accountability, https://www.govinfo.gov/content/pkg/BUDGET-2026-APP/pdf/BUDGET-2026-APP-2-14.pdf.
151. Perry Stein et al., "FBI dispatching agents to D.C. streets as Trump weighs calling National Guard," *The Washington Post*, August 10, 2025, https://www.washingtonpost.com/dc-md-va/2025/08/10/dc-crime-trump-crackdown/.
152. Perry Stein, "A quarter of FBI agents are assigned to immigration enforcement, per FBI data," *The Washington Post*, October 8, 2025.
153. Ibid.
154. Sam Sabin. "Exclusive: One-third of top U.S. cyber force has left since Trump took office," Axios, June 3, 2025, https://www.axios.com/2025/06/03/cisa-staff-layoffs-resignations-trump-cuts.
155. United States Attorney's Office, Southern District of Florida, "California Woman Sentenced to 50 Months in Prison for Conspiring to Illegally Export Fight Jet Engines and Unmanned Aerial Vehicle to China," August 19, 2016, https://www.justice.gov/usao-sdfl/pr/california-woman-sentenced-50-months-prison-conspiring-illegally-export-fighter-jet.
156. Congressional Research Service, "Made in China 2025 and Industrial Policies: Issues for Congress," 2024.
157. https://www.justice.gov/usao-sdfl/pr/california-woman-sentenced-50-months-prison-conspiring-illegally-export-fighter-jet.
158. David J. Bier, "ICE Has Diverted Over 25,000 Officers from Their Jobs," Cato, September 3, 2025, https://www.cato.org/blog/ice-has-diverted-over-25000-officers-their-jobs.
159. U.S. Department of Justice, "Superseding Indictment Charges Chinese National in Relation to Alleged Plan to Steal Proprietary AI Technology," February 4, 2025, https://www.justice.gov/opa/pr/superseding-indictment-charges-chinese-national-relation-alleged-plan-steal-proprietary-ai; *United States of America v. Linwei Ding a.k.a Leon Ding*, https://www.justice.gov/opa/media/1388341/dl?inline.
160. Julian E. Barnes, "Chinese Intelligence May Be Trying to Recruit Fired U.S. Officials," *The New York Times*, April 8, 2025, https://www.nytimes.com/2025/04/08/us/politics/chinese-intelligence-fired-us-workers.html.
161. Jennifer Jett and Peter Guo, "U.S. will 'aggressively' revoke Chinese students' visas, Rubio says, NBC, May 28, 2025, https://www.nbcnews.com/world/asia/us-will-aggressively-revoke-chinese-students-visas-rubio-says-rcna209637.
162. National Security Memorandum/NSM-12, "National Security Memorandum on the President's Intelligence Priorities," July 12, 2022, https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/07/12/national-security-memorandum-on-the-presidents-intelligence-priorities/; Intelligence Community Directive 204, "National Intelligence Priorities Framework."
163. Intelligence Community Directive 204, "National Intelligence Priorities Framework," https://www.dni.gov/files/documents/ICD/ICD_204_National_Intelligence_Priorities_Framework_U_FINAL-SIGNED.pdf.