

**INFORMATION ABOUT THE DEPARTMENT OF JUSTICE'S CHINA
INITIATIVE AND A COMPILATION OF CHINA-RELATED
PROSECUTIONS SINCE 2018**

Last Updated July 10, 2020

Background

About 80 percent of all economic espionage prosecutions brought by the U.S. Department of Justice (DOJ) allege conduct that would benefit the Chinese state, and there is at least some nexus to China in around 60 percent of all trade secret theft cases.

The Department of Justice's China Initiative reflects the strategic priority of countering Chinese national security threats and reinforces the President's overall national security strategy. The Initiative was launched against the background of previous findings by the Administration concerning China's practices. In March 2018, the Office of the U.S. Trade Representative announced the results of an investigation of China's trade practices under Section 301 of the Trade Act of 1974. It concluded, among other things, that a combination of China's practices are unreasonable, including its outbound investment policies and sponsorship of unauthorized computer intrusions, and that "[a] range of tools may be appropriate to address these serious matters."

In June 2018, the White House Office of Trade and Manufacturing Policy issued a report on "How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World," documenting "the two major strategies and various acts, policies, and practices Chinese industrial policy uses in seeking to acquire the intellectual property and technologies of the world and to capture the emerging high- technology industries that will drive future economic growth."

In addition to identifying and prosecuting those engaged in trade secret theft, hacking, and economic espionage, the Initiative focuses on protecting our critical infrastructure against external threats through foreign direct investment and supply chain compromises, as well as combatting covert efforts to influence the American public and policymakers without proper transparency.

The China Initiative is led by the Department's National Security Division (NSD), which is responsible for countering nation-state threats to the United States.

China Initiative Leadership and Steering Committee Members

- [John C. Demers](#) , Assistant Attorney General for National Security, Chair
- [David L. Anderson](#), U.S. Attorney, Northern District of California
- [Brian A. Benczkowski](#), Assistant Attorney General, Criminal Division
- [John Brown](#), Executive Assistant Director, National Security Branch, FBI
- [Erin Nealy Cox](#), U.S. Attorney, Northern District of Texas
- [Richard P. Donoghue](#), U.S. Attorney, Eastern District of New York
- [Andrew E. Lelling](#), U.S. Attorney, District of Massachusetts
- [Jay E. Town](#), U.S. Attorney, Northern District of Alabama

Components of Initiative

The Attorney General set the following goals for the Initiative:

- Identify priority trade secret theft cases, ensure that investigations are adequately resourced, and work to bring them to fruition in a timely manner and according to the facts and applicable law;
- Develop an enforcement strategy concerning non-traditional collectors (e.g., researchers in labs, universities and the defense industrial base) that are being coopted into transferring technology contrary to U.S. interests;
- Educate colleges and universities about potential threats to academic freedom and open discourse from influence efforts on campus;

- Apply the Foreign Agents Registration Act to unregistered agents seeking to advance China's political agenda, bringing enforcement actions when appropriate;
- Equip the nation's U.S. Attorneys with intelligence and materials they can use to raise awareness of these threats within their Districts and support their outreach efforts;
- Implement the Foreign Investment Risk Review Modernization Act (FIRRMA) for DOJ (including by working with Treasury to develop regulations under the statute and prepare for increased workflow);
- Identify opportunities to better address supply chain threats, especially those impacting the telecommunications sector, prior to the transition to 5G networks;
- Identify Foreign Corrupt Practices Act (FCPA) cases involving Chinese companies that compete with American businesses;
- Increase efforts to improve Chinese responses to requests under the Mutual Legal Assistance Agreement (MLAA) with the United States; and
- Evaluate whether additional legislative and administrative authorities are required to protect our national assets from foreign economic aggression.

China-Related Cases Examples

Thursday, July 9, 2020

[Researcher Charged with Illegally Using U.S. Grant Funds to Develop Scientific Expertise for China](#)

A rheumatology professor and researcher with strong ties to China has been ordered held without bond to face a charge of grant fraud for not disclosing that he was engaged in a sophisticated scheme to use approximately \$4.1 million in grants from the National Institutes of Health (NIH) to develop China's expertise in the areas of rheumatology and immunology. He is also charged with making false statements about maintaining employment in China at the same time he was employed at universities in the United States, including The Ohio State University.

Friday, June 26, 2020

[Chinese Citizen Convicted of Economic Espionage, Theft of Trade Secrets, and Conspiracy](#)

Hao Zhang, 41, of China, was found guilty of economic espionage, theft of trade secrets, and conspiring to commit both offenses today, announced the Department of Justice. The ruling was handed down by the Honorable Edward J. Davila, U.S. District Judge, following a four-day bench trial.

Wednesday, June 17, 2020

[Team Telecom Recommends that the FCC Deny Pacific Light Cable Network System's Hong Kong Undersea Cable Connection to the United States](#)

Team Telecom today recommended to the Federal Communications Commission (FCC), based on national security concerns, that the FCC partially deny the Pacific Light Cable Network (PLCN) subsea cable system application, to the extent it seeks a direct connection between the United States and Hong Kong.

Tuesday, June 9, 2020

[Harvard University Professor Indicted on False Statement Charges](#)

The former Chair of Harvard University's Chemistry and Chemical Biology Department was indicted today on charges of making false statements to federal authorities regarding his participation in China's Thousand Talents Program. Dr. Charles Lieber, 61, has been indicted by a federal grand jury on two counts of making false statements and will be arraigned in federal court in Boston at a later date. Lieber was arrested on Jan. 28, 2020, and charged by criminal complaint.

Thursday, May 14, 2020

[Former Cleveland Clinic Employee and Chinese "Thousand Talents" Participant Arrested for Wire Fraud](#)

Assistant Attorney General for National Security John C. Demers, U.S. Attorney Justin E. Herdman of

the Northern District of Ohio, and FBI Cleveland Special Agent in Charge Eric B. Smith announced a former Cleveland Clinic employee was arrested yesterday without incident by law enforcement and had his initial court appearance today. Dr. Wang, a former Cleveland Clinic Foundation (CCF) employee, is charged with false claims and wire fraud related to more than \$3.6 million in grant funding that Dr. Wang and his research group received from the National Institutes of Health (NIH).

Monday, May 11, 2020

[University of Arkansas Professor Arrested for Wire Fraud](#)

Assistant Attorney General for National Security John C. Demers, David Clay Fowlkes, Acting U.S. Attorney for the Western District of Arkansas, and FBI Special Agent in Charge Diane Upchurch of the FBI Little Rock Field Office announced today that Simon Saw-Teong Ang, 63, of Fayetteville, Arkansas, was arrested on Friday, May 8, 2020, on charges related to Wire Fraud. The complaint and complaint affidavit were unsealed this evening after Ang's initial appearance in court before The Honorable Timothy L. Brooks at the United States District Court in Fayetteville.

Monday, May 11, 2020

[Former Emory University Professor and Chinese "Thousand Talents" Participant Convicted and Sentenced for Filing a False Tax Return](#)

On May 8, 2020, Dr. Xiao-Jiang Li, 63, of Atlanta, Georgia, pleaded guilty to a criminal information charging him with filing a false tax return and has been sentenced by a United States District Judge on the same day. Dr. Li, a former Emory University professor and Chinese Thousand Talents Program participant, worked overseas at Chinese Universities and did not report any of his foreign income on his federal tax returns.

Thursday, April 9, 2020

[Executive Branch Agencies Recommend the FCC Revoke and Terminate China Telecom's Authorizations to Provide International Telecommunications Services in the United States](#)

Today, interested Executive Branch agencies¹ unanimously recommended that the Federal Communications Commission (FCC) revoke and terminate China Telecom (Americas) Corp.'s authorizations to provide international telecommunications services to and from the United States. China Telecom is the U.S. subsidiary of a People's Republic of China (PRC) state-owned telecommunications company.

Tuesday, March 17, 2020

[Hayward Resident Sentenced to Four Years for Acting as an Agent of the People's Republic of China](#)

Xuehua (Edward) Peng aka Edward Peng was sentenced yesterday to 48 months in prison, and ordered to pay a \$30,000 fine for acting as an agent of the People's Republic of China's Ministry of State Security (MSS) in connection with a scheme to conduct pickups known as "dead drops" and transport Secure Digital (SD) cards from a source in the United States to the MSS operatives in China, announced the Department of Justice.

Tuesday, March 10, 2020

[Former West Virginia University Professor Pleads Guilty to Fraud That Enabled Him to Participate in the People's Republic of China's "Thousand Talents Plan"](#)

Dr. James Patrick Lewis, of Fairview, West Virginia, has admitted to a fraud charge involving West Virginia University, the Department of Justice announced. Lewis, age 54, pleaded guilty to a one-count information charging him with "Federal Program Fraud." From 2006 to August 2019, Lewis was a tenured professor at West Virginia University in the physics department, specializing in molecular reactions used in coal conversion technologies. In July 2017, Lewis entered into a contract of employment with the

¹ For purposes of the recommendation, the Executive Branch agencies included the Departments of Justice, Homeland Security, Defense, State, Commerce, and the United States Trade Representative.

People's Republic of China through its "Global Experts 1000 Talents Plan." China's Thousand Talents Plan is one of the most prominent Chinese Talent recruit plans that are designed to attract, recruit, and cultivate high-level scientific talent in furtherance of China's scientific development, economic prosperity and national security. These talent programs seek to lure overseas talent and foreign experts to bring their knowledge and experience to China and reward individuals for stealing proprietary information.

Thursday, February 27, 2020

[Researcher at University Arrested for Wire Fraud and Making False Statements About Affiliation with a Chinese University](#)

Anming Hu, an Associate Professor in the Department of Mechanical, Aerospace and Biomedical Engineering at the University of Tennessee, Knoxville was arrested on a federal indictment and charged with three counts of wire fraud and three counts of making false statements.

Thursday, February 27, 2020

[Chinese National Sentenced for Stealing Trade Secrets Worth \\$1 Billion](#)

A former associate scientist was sentenced to 24 months in federal prison in federal court for stealing proprietary information worth more than \$1 billion from his employer, a U.S. petroleum company.

Thursday, February 13, 2020

[Chinese Telecommunications Conglomerate Huawei and Subsidiaries Charged in Racketeering Conspiracy and Conspiracy to Steal Trade Secrets](#)

A superseding indictment was returned in Brooklyn, New York, charging Huawei Technologies Co. Ltd. (Huawei), the world's largest telecommunications equipment manufacturer and two U.S. subsidiaries with conspiracy to violate the Racketeer Influenced and Corrupt Organizations Act (RICO). The original indictment against Huawei for financial fraud was filed in January 2019 (see below).

Tuesday, February 11, 2020

[American Businessman Who Ran Houston-Based Subsidiary of Chinese Company Sentenced To Prison for Theft of Trade Secrets](#)

The head of a Houston-based company that was the subsidiary of a Chinese company that developed stolen trade secrets was sentenced to 16 months in prison and ordered to forfeit more than \$330,000 in the District of Columbia.

Monday, February 10, 2020

[Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax](#)

A federal grand jury in Atlanta returned an indictment charging four members of the Chinese People's Liberation Army (PLA) with hacking into the computer systems of the credit reporting agency Equifax and stealing Americans' personal data and Equifax's valuable trade secrets.

Tuesday, January 28, 2020

[Harvard University Department Chair Charged with Making a Materially False, Fictitious and Fraudulent Statement Regarding Work for China's Thousand Talents Plan](#)

Dr. Charles Lieber, 60, Chair of the Department of Chemistry and Chemical Biology at Harvard University, was arrested and charged by criminal complaint with making a materially false, fictitious and fraudulent statement regarding his affiliation with China's Thousand Talents Plan and his work for a Chinese university. According to court documents, since 2008, Dr. Lieber who has served as the Principal Investigator of the Lieber Research Group at Harvard University, which specialized in the area of nanoscience, has received more than \$15,000,000 in grant funding from the National Institutes of Health (NIH) and Department of Defense (DOD). These grants require the disclosure of significant foreign financial conflicts of interest, including financial support from foreign governments or foreign entities.

Tuesday, January 28, 2020

[Visiting Student Charged with Visa Fraud, Making False Statements, Acting as an Agent of a Foreign Government and Conspiracy](#)

Yanqing Ye, 29, a Chinese national, was charged in an indictment with one count each of visa fraud, making false statements, acting as an agent of a foreign government without prior notification to the Attorney General, and conspiracy. According to the indictment, Ye is a Lieutenant of the People's Liberation Army (PLA), the armed forces of the People's Republic of China, and member of the Chinese Communist Party (CCP). On her J-1 student visa application, Ye falsely identified herself as a "student" and lied about her ongoing military service at the National University of Defense Technology (NUDT), a top military academy directed by the CCP. It is further alleged that, while studying at Boston University's Department of Physics, Chemistry and Biomedical Engineering, Ye continued to work as a PLA Lieutenant completing numerous assignments from PLA officers such as conducting research, assessing U.S. military websites, and sending U.S. documents and information to China.

Tuesday, January 28, 2020

[Cancer Researcher from China Charged with Smuggling and False Statements After Being Caught at the Airport with Twenty-one Vials of Stolen Biological Research Material](#)

Zaosong Zheng, 30, a Chinese national, was arrested at Boston's Logan International Airport, and charged by criminal complaint with attempting to smuggle twenty-one vials of biological research to China. Zheng was later indicted on one count of smuggling goods from the United States and one count of making false, fictitious or fraudulent statements. In August 2018, Zheng entered the United States on a J-1 visa and conducted cancer-cell research at Beth Israel Deaconess Medical Center in Boston. It is alleged that Zheng stole twenty-one vials of biological research and attempted to smuggle them out of the United States aboard a flight destined for China. Federal officers at Logan Airport discovered the vials hidden in a sock inside one of Zheng's bags, and not properly packaged. Zheng lied to officers about the contents of his luggage, but later admitted he had stolen the vials from a lab at Beth Israel. Zheng stated that he intended to bring the vials to China to use them to conduct research in his own laboratory and publish the results under his own name.

Thursday, December 19, 2019

[Department of Justice Reaches \\$5.5 Million Settlement with Van Andel Research Institute to Resolve Allegations of Undisclosed Chinese Grants to Two Researchers](#)

The Department of Justice announced today that Van Andel Research Institute (VARI) has agreed to pay \$5,500,000.00 to resolve allegations that it violated the False Claims Act by submitting federal grant applications and progress reports to the National Institutes of Health (NIH), in which VARI failed to disclose Chinese government grants that funded two VARI researchers. The settlement further resolves allegations that, in a December 2018 letter, VARI made certain factual representations to NIH with deliberate ignorance or reckless disregard for the truth regarding the Chinese grants.

Friday, November 22, 2019

[Former CIA Officer Sentenced for Conspiracy to Commit Espionage](#)

A former Central Intelligence Agency (CIA) case officer was sentenced to 19 years in prison for conspiring to communicate, deliver and transmit national defense information to the People's Republic of China. According to court documents, Jerry Chun Shing Lee, 55, left the CIA in 2007 and began residing in Hong Kong. In April 2010, two Chinese intelligence officers approached Lee and offered to pay him for national defense information he had acquired as a CIA case officer. The intelligence officers also told Lee they had prepared for him a gift of \$100,000 cash, and they offered to take care of him "for life" in exchange for his cooperation.

Thursday, November 21, 2019

[Chinese National Who Worked at Monsanto Indicted on Economic Espionage Charges](#)

Haitao Xiang, 42, formerly of Chesterfield, Missouri, was indicted today by a federal grand jury on one count of conspiracy to commit economic espionage, three counts of economic espionage, one

count of conspiracy to commit theft of trade secrets, and three counts of theft of trade secrets. According to the indictment, Xiang was selected to be a member of a Chinese government Talent Plan, and, within a year, quit his job, and sought to take proprietary farming software to China.

Thursday, November 14, 2019

[Two Former Executives of the China Subsidiary of a Multi-Level Marketing Company Charged for Scheme to Pay Foreign Bribes and Circumvent Internal Accounting Controls](#)

The former head of the Chinese subsidiary of a publicly traded international multi-level marketing company and the former head of the external affairs department of the Chinese subsidiary of the same company were charged for their roles in a scheme to violate the anti-bribery and the internal control provisions of the Foreign Corrupt Practices Act (FCPA).

Friday, November 1, 2019

[U.S. Navy Officer, His Wife, and Two Chinese Nationals Charged with Conspiring to Smuggle Military Style Inflatable Boats and Evinrude Military Outboard Motors to China](#)

Four individuals, including two Chinese nationals, an active-duty United States Navy officer, and his wife, indicted on charges relating to a conspiracy to unlawfully smuggle military-style inflatable boats, with Evinrude MFE military outboard motors, to the People's Republic of China. The Navy officer and two other defendants have also been charged with conspiring to violate firearms law, and the Navy officer has been charged with an additional firearms-related offense and with making false official statements.

Friday, October 18, 2019

[Chinese National Sentenced to 40 Months in Prison for Conspiring to Illegally Export Military- and Space-Grade Technology from the United States to China](#)

Tao Li, a 39-year-old Chinese national, was sentenced to 40 months in prison, followed by three years of supervised release after pleading guilty to conspiring to export military and space-grade technology to the People's Republic of China without a license, in violation of the International Emergency Economic Powers Act (IEEPA), which makes certain unauthorized exports illegal.

Tuesday, September 24, 2019

[Former Intelligence Officer Convicted of Attempted Espionage Sentenced to 10 Years in Federal Prison](#)

Ron Rockwell Hansen, 60, of Utah, a former Defense Intelligence Agency officer, who pleaded guilty to attempting to communicate, deliver, or transmit information involving the national defense of the United States to the People's Republic of China, was sentenced to 10 years in federal prison.

Monday, September 30, 2019

[Northern California Resident Charged with Acting as an Illegal Agent](#)

Xuehua Peng, also known as Edward Peng, was charged for acting as an illegal foreign agent for delivering classified United States national security information to officials of the People's Republic of China's Ministry of State Security (MSS). The MSS is the intelligence and security agency for China and is responsible for counterintelligence, foreign intelligence and political security. MSS has broad powers in China to conduct espionage both domestically and abroad.

Monday, September 16, 2019

[Chinese Government Employee Charged in Manhattan Federal Court with Participating in Conspiracy to Fraudulently Obtain U.S. Visas](#)

Zhongsan Liu was arrested and charged for his involvement in a conspiracy to fraudulently obtain U.S. research visas for PRC government employees seeking to recruit U.S. experts to China.

Monday, September 16, 2019

[Couple Who Worked at Local Research Institute for 10 Years Charged with Stealing Trade Secrets, Wire Fraud](#)

A former Dublin, Ohio couple has been charged with stealing exosome-related trade secrets concerning the research, identification and treatment of a range of pediatric medical conditions.

Wednesday, August 21, 2019

[University of Kansas Researcher Indicted for Fraud for Failing to Disclose Conflict of Interest with Chinese University](#)

Feng “Franklin” Tao, an associate professor at Kansas University, was indicted on federal charges for concealing the fact he was a full-time employee for Fuzhou University, in China, while doing research at KU that was funded by the U.S. government. He was charged with one count of wire fraud and three counts of program fraud.

Tuesday, July 23, 2019

[Four Chinese Nationals and Chinese Company Indicted for Conspiracy to Defraud the United States and Evade Sanctions](#)

A federal grand jury charged four Chinese nationals and a Chinese company with violating the International Emergency Economic Powers Act (IEEPA), conspiracy to violate IEEPA and defraud the U.S.; conspiracy to violate, evade and avoid restrictions imposed under the Weapons of Mass Destruction Proliferators Sanctions Regulations; and conspiracy to launder monetary instruments. The company is alleged to have tried to obscure illicit financial dealings on behalf of sanctioned North Korean entities that were involved in the proliferation of weapons of mass destruction.

Thursday, July 11, 2019

[Newly Unsealed Federal Indictment Charges Software Engineer with Taking Stolen Trade Secrets to China](#)

Xudong Yao, also known as “William Yao,” a software engineer at a suburban Chicago locomotive manufacturer, was charged with nine counts of theft of trade secrets for allegedly stealing proprietary information from the company and taking it to China.

Tuesday, July 9, 2019

[Former State Department Employee Sentenced for Conspiring with Chinese Agents](#)

Candace Marie Clairborne, a former employee of the U.S. Department of State, was sentenced to 40 months in prison, three years of supervised release, and a fine of \$40,000. Clairborne was found guilty of conspiracy to defraud the United States by lying to law enforcement and background investigators, and hiding her extensive contacts with, and gifts from, agents of the People’s Republic of China, which were provided in exchange for internal documents from the U.S. State Department.

Tuesday, July 2, 2019

[Electrical Engineer Convicted of Conspiring to Illegally Export to China Semiconductor Chips with Missile Guidance Applications](#)

Yi-Chi Shih, an electrical engineer, was found guilty of multiple criminal charges, including a scheme to illegally obtain integrated circuits with military applications that were later exported to China without the required export license. After a six-week trial, Shih was found guilty of conspiracy to violate the International Emergency Economic Powers Act, a federal law that makes certain unauthorized exports illegal.

Friday, May 17, 2019

[Former CIA Officer Sentenced to Prison for Espionage](#)

Former U.S. Intelligence officer Kevin Patrick Mallory was convicted under the Espionage Act for conspiracy to transmit national defense information to an agent of the People’s Republic of China. He was sentenced to 20 years in prison followed by five years of supervised release.

Thursday, May 9, 2019

[Member of Sophisticated China-Based Hacking Group Indicted for Series of Computer Intrusions, Including 2015 Data Breach of Health Insurer Anthem Inc. Affecting Over 78 Million People](#)

A federal grand jury returned an indictment unsealed in Indianapolis, Indiana, charging a Chinese national as part of an extremely sophisticated hacking group operating in China and targeting large businesses in the United States, including a computer intrusion and data breach of Indianapolis-based health insurer Anthem Inc.

Tuesday, April 23, 2019

[Former GE Engineer and Chinese Businessman Charged with Economic Espionage and Theft of GE's Trade Secrets](#)

An indictment charged Xiaoqing Zheng and Zhaoxi Zhang with economic espionage and conspiring to steal General Electric's (GE's) trade secrets relating to its turbine technology, knowing and intending that the stolen trade secrets would be used to benefit the People's Republic of China. The 14-count indictment alleged Zheng, while employed at GE Power & Water, exploited his access by stealing multiple electronic files and transferring them to Zhang, his business partner in China.

Wednesday, April 17, 2019

[Former Manager for International Airline Pleads Guilty to Acting as an Agent of the Chinese Government](#)

Ying Lin, a former manager with an international air carrier headquartered in the People's Republic of China, pleaded guilty to acting as an agent of the PRC, without prior notification to the Attorney General, by working at the direction and control of military officers assigned to the Permanent Mission of the PRC to the United Nations. Lin transported packages from John F. Kennedy International Airport to the PRC at the orders of the Chinese military officers, in violation of Transportation Security Administration regulations. Lin was subsequently sentenced to probation.

Friday, February 15, 2019

[Chinese National Sentenced to Prison for Selling Counterfeit Computer Parts](#)

Ruiyang Li, a man from Beijing, China, was sentenced to serve 54 months in federal prison for directing the shipment of counterfeit computer-networking equipment into the Southern District of Texas.

Thursday, February 14, 2019

[One American and One Chinese National Indicted in Tennessee for Conspiracy to Commit Theft of Trade Secrets and Wire Fraud](#)

A grand jury returned an indictment against Xiaorong ("Shannon") You and Liu Xiangchen, for conspiracy to steal trade secrets related to formulations for bisphenol-A-free coatings. The indictment alleges that You, Liu, and a third co-conspirator planned for You to exploit her employment with her American employers to steal trade secrets and provide the information for the economic benefit of the Chinese company that Liu managed. Liu's company planned to manufacture and profit from the products developed using the stolen trade secrets.

Monday, January 28, 2019

[Chinese Telecommunications Device Manufacturer and its U.S. Affiliate Indicted for Theft of Trade Secrets, Wire Fraud, and Obstruction of Justice](#)

A 10-count indictment, unsealed in the Western District of Washington, charged Huawei Device Co., Ltd. and Huawei Device Co. USA with theft of trade secrets conspiracy, attempted theft of trade secrets, seven counts of wire fraud, and one count of obstruction of justice. The indictment, returned by a grand jury, details Huawei's efforts to steal trade secrets from T-Mobile USA and then obstruct justice when T-Mobile threatened to sue Huawei in U.S. District Court. The alleged conduct described in the indictment occurred from 2012 to 2014, and includes an internal Huawei announcement that the

company was offering bonuses to employees who succeeded in stealing confidential information from other companies.

Monday, January 28, 2019

[Chinese Telecommunications Conglomerate Huawei and Huawei CFO Wanzhou Meng Charged With Financial Fraud](#)

A 13-count indictment, unsealed in a federal court in Brooklyn, New York, charged four defendants — Huawei Technologies Co. Ltd., Huawei Device USA Inc., Skycom Tech Co. Ltd., and Huawei's Chief Financial Officer Wanzhou Meng — with various crimes. Huawei and Skycom are charged with bank fraud, and conspiracy to commit bank fraud, wire fraud and conspiracy to commit wire fraud, violations of the International Emergency Economic Powers Act (IEEPA), conspiracy to violate IEEPA, and conspiracy to commit money laundering. Huawei and Huawei USA are charged with conspiracy to obstruct justice related to the grand jury investigation in the Eastern District of New York. Meng is charged with bank fraud, wire fraud, and conspiracies to commit bank and wire fraud.

Thursday, December 20, 2018

[Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information](#)

In the Southern District of New York, the Department unsealed an indictment charging Chinese nationals Zhu Hua and Zhang Shilong with conspiracy to commit computer intrusions, conspiracy to commit wire fraud, and aggravated identity theft. As alleged, the defendants, through their involvement in a hacking group associated with the Chinese Ministry of State Security, from 2006 to in or about 2018, conducted global campaigns of computer intrusions targeting, among other data, intellectual property and confidential business and technological information at managed service providers, which are companies that remotely manage the information technology infrastructure of businesses and governments around the world, including in the United States.

Wednesday, December 5, 2018

[Former Head of Organization Backed by Chinese Energy Conglomerate Convicted of International Bribery, Money Laundering Offenses](#)

Chi Ping Patrick Ho, the head of the China Energy Fund Committee, a nongovernmental organization, was convicted on seven counts for his participation in a multi-year, multimillion-dollar scheme to bribe top officials of Chad and Uganda in exchange for business advantages for a Chinese oil and gas company. After a one-week jury trial, Ho was found guilty of one count of conspiring to violate the Foreign Corrupt Practices Act (FCPA), four counts of violating the FCPA, one count of conspiring to commit international money laundering, and one count of committing international money laundering.

Thursday, November 1, 2018

[PRC State-Owned Company, Taiwan Company, and Three Individuals Charged With Economic Espionage](#)

A federal grand jury indicted a state-owned enterprise of the People's Republic of China (PRC), a Taiwan company, and three individuals, charging them with crimes related to a conspiracy to steal, convey, and possess stolen trade secrets of an American semiconductor company for the benefit of a company controlled by the PRC government. All of the defendants are charged with a conspiracy to commit economic espionage, among other crimes. In addition, the United States filed a civil lawsuit seeking to enjoin the export to the United States of any products manufactured by UMC or Jinhua that were created using the trade secrets at issue.

Tuesday, October 30, 2018

[Chinese Intelligence Officers and their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years](#)

Chinese intelligence officers, and those working under their direction, which included hackers and co-opted company insiders, conducted or otherwise enabled repeated intrusions into private companies'

computer systems in the United States and abroad, for over five years. The conspirators' ultimate goal was to steal, among other data, intellectual property and confidential business information, including information related to a turbofan engine used in commercial airliners.

Wednesday, October 10, 2018

[Chinese Intelligence Officer Charged with Economic Espionage Involving Theft of Trade Secrets from Leading U.S. Aviation Companies](#)

A Chinese Ministry of State Security (MSS) operative, Yanjun Xu, also known as Qu Hui and Zhang Hui, was arrested and charged with conspiring and attempting to commit economic espionage and theft of trade secrets from multiple U.S. aviation and aerospace companies. Xu was extradited to the United States in October 2018. Xu is a Deputy Division Director with the MSS's Jiangsu State Security Department, Sixth Bureau.

Tuesday, September 25, 2018

[Chinese National Arrested for Allegedly Acting Within the United States as an Illegal Agent of the People's Republic of China](#)

Ji Chaoqun, a Chinese citizen residing in Chicago, was arrested for allegedly acting within the United States as an illegal agent of the People's Republic of China. Ji was charged with one count of knowingly acting in the United States as an agent of a foreign government without prior notification to the Attorney General. Ji was tasked with providing a high-level intelligence officer in the Jiangsu Province with biographical information on eight individuals for possible recruitment by the MSS.

Wednesday, April 4, 2018

[Chinese Scientist Sentenced to Prison in Theft of Engineered Rice](#)

Weiqiang Zhang, a Chinese national and U.S. Legal Permanent Resident, was sentenced to 121 months in a federal prison for conspiring to steal samples of rice seeds from a Kansas biopharmaceutical research facility. Zhang acquired, without authorization, hundreds of rice seeds produced by his employer, Ventria Bioscience. The seeds were found by U.S. Customs and Border Protection officers in the luggage of Zhang's China-based colleagues, as they prepared to leave for China from the United States.