

NOTABLE DEVELOPMENTS

- [September 25, 2024](#): The House Committee on Homeland Security (CHS) passed on a bipartisan basis H.R. 9668, the SHIELD Against CCP Act and H.R. 9769, the Strengthening Cyber¹ Resilience Against State-Sponsored Threats Act.
- [September 16, 2024](#): CHS and the Select Committee on the Chinese Communist Party released a joint investigative report exposing the rising threat to U.S. economic and homeland security posed by the Chinese Communist Party (CCP).
- [June 20, 2024](#): CHS and the Committee on Energy and Commerce urged the Department of Homeland Security and Department of Energy to declassify information relating to potential national risks posed by drones that have been manufactured in the People's Republic of China (PRC).
- [June 12, 2024](#): CHS passed on a bipartisan basis H.R. 8631, the Decoupling from Foreign Adversarial Battery Dependency Act. [On September 9, 2024](#), H.R. 8631 passed on the House floor.
- [April 10, 2024](#): CHS passed on a bipartisan basis H.R. 7443, the Countering Transnational Repression² Act, H.R. 7433, the Law Enforcement Support and Counter Transnational Repression Act, and H.R. 7439, the Strengthening State and Local Efforts to Counter Transnational Repression Act. [On January 17, 2024](#), the Subcommittee on Counterterrorism, Law Enforcement, and Intelligence heard harrowing testimony about the threat of transnational repression, including testimony from American citizens and dissidents directly impacted by the PRC's brazen acts of transnational repression.
- [November 8, 2023](#): CHS passed H.R. 1516, the DHS Restrictions on Confucius Institutes and Chinese Entities of Concern Act. [On September 10, 2024](#), H.R. 1516 passed on the House floor.
- [May 17, 2023](#): CHS passed H.R. 1501, the Unmanned Aerial Security Act. [On July 27, 2023](#), H.R. 1501 passed on the House floor.
- [April 17, 2023](#): According to the Department of Justice (DOJ), the PRC established a secret physical presence in Manhattan, New York to track and intimidate dissidents and those critical of the PRC.³
- [March 9, 2023](#): Bill Evanina, former Senate-confirmed Director of the National Counterintelligence and Security Center testified before the Subcommittee on Counterterrorism, Law Enforcement, and Intelligence that China "continues to utilize non-traditional collectors to conduct a plurality of their nefarious efforts here in the U.S. due to their successful ability to hide in plain sight. The non-traditional collectors, serving as engineers, businesspersons, academics, and students are shrouded in legitimate work and research, and oftentimes become unwitting tools for the CCP and its intelligence apparatus."

¹ According to [testimony](#) by FBI Director Wray: "if each one of the FBI's cyber agents and intelligence analysts focused exclusively on the China threat, China's hackers would still outnumber FBI cyber personnel by at least 50 to 1."

² According to [testimony](#) before the Subcommittee on Counterterrorism, Law Enforcement, and Intelligence, from 2014 through 2022, the Freedom House "has collected information on 854 direct, physical incidents (assassination, kidnapping, assault, detention, or deportation) of transnational repression around the world, committed by 38 governments in 91 countries. During this time, 13 states have engaged in assassinations abroad, and 30 have conducted renditions." According to the Freedom House, the PRC is a top perpetrator of transnational repression in the world.

³ The PRC's illegal operation of overseas police service stations is extensive in more than 50 countries, including the United States. See Safeguard Defenders 2022 Report *Patrol and Persuade*.

- [January 31, 2022](#): Christopher Wray, the Director of the Federal Bureau of Investigation (FBI) stated that “over 2,000” of the FBI’s investigations “are focused on the Chinese government trying to steal our information and technology” and that the FBI opens “new cases to counter their intelligence operations, about every 12 hours or so.” Director Wray also [stated](#) that “the greatest long-term threat to our nation’s information and intellectual property, and to our economic vitality, is the counterintelligence and economic espionage threat from China.”
- According to a survey conducted by the Center for Strategic and International Studies, between 2000 and 2023, there have been [224 reported incidents](#) of Chinese espionage⁴ directed at the United States.⁵
- According to a [May 2021](#) report by the Intelligence and National Security Alliance, 20% of U.S. companies claim that entities related to the PRC have stolen their intellectual property (IP). PRC [theft of U.S. IP](#) is extensive, estimating between \$300 billion and \$600 billion annually. This is about \$4,000 to \$6,000 per American family of four after paying taxes.

CCP-RELATED ESPIONAGE AND ACTS OF TRANSNATIONAL REPRESSION IN THE HOMELAND: RECENT DEVELOPMENTS⁶

The government of China and the Chinese Communist Party (CCP) seriously threatens the economic well-being, homeland security, and democratic values of the United States (U.S.). Cases of Chinese espionage throughout the U.S. have expanded rapidly with Chinese nationals and non-Chinese individuals acting on behalf of the People’s Republic of China (PRC) allegedly committing a variety of forms of espionage including but not limited to, government, military, and economic espionage.⁷

2024

- [January 31, 2024](#): Four PRC nationals—Baoxia LIU, Yiu Wa YUNG, Yongxin LI, and Yanlai ZHONG—were indicted in the District of Columbia for their involvement in a conspiracy to unlawfully export and smuggle U.S.-origin electronic components to Iran

⁴ According to the PRC’s new National Intelligence Law passed in 2017, all Chinese citizens including those who were born as American citizens, are required to support, assist, and cooperate with state intelligence work. Article 7 of the PRC National Intelligence Law obligates Chinese individuals, organizations, and institutions to support national intelligence work in every aspect. Article 14 provides the Chinese intelligence agencies the authority to demand such cooperation.

⁵ [69% of incidents](#) were reported after Xi took office; [46% of incidents](#) involved cyber espionage, typically by state-affiliated actors; [29% of incidents](#) sought to acquire military technology; and [54% of incidents](#) aimed to acquire commercial technologies. Of these reported incidents: [49% involved](#) Chinese military or government employees; [41% involved](#) private Chinese citizens; and [10% involved](#) non-Chinese actors, often U.S. persons recruited by Chinese officials.

⁶ Unless otherwise specified, incidents included in this report span approximately January 2021, through October 2024. All figures are based on open-source and government data compiled and analyzed by the Majority Staff of the House Homeland Security Committee, Subcommittee on Counterterrorism, Law Enforcement, and Intelligence.

⁷ In general, economic espionage means: (1) whoever knowingly performs targeting or acquisition of trade secrets to (2) knowingly benefit any foreign government, foreign instrumentality, or foreign agent. 18 U.S.C. § 1831. According to the FBI, “about 80 percent of economic espionage prosecutions 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.” Information About the Department of Justice’s China Initiative and a Compilation of China-Related Prosecutions Since 2018, DEP’T OF JUST., <https://www.justice.gov/archives/nsd/information-about-department-justice-s-china-initiative-and-compiled-china-related> (last updated Nov. 19, 2021).

over several years. The defendants allegedly utilized front companies in the PRC to funnel dual-use items, including those used for military applications, to Iranian entities affiliated with the Islamic Revolutionary Guard Corps.

- [January 25, 2024](#): Xiaolei WU, a PRC citizen and Berklee College of Music student, was convicted in the District of Massachusetts for threatening and stalking an individual who posted a flier on the Berklee campus in support of democracy in the PRC. The jury found Wu guilty of cyberstalking and interstate transmissions of threatening communication after he harassed, threatened, and intimidated the victim online.
- [January 8, 2024](#): Petty Officer Wenheng Zhao, of California, was sentenced to 27 months in prison for transmitting sensitive military information to a PRC agent in exchange for bribery payments.
- [February 5, 2024](#): Chenguang Gong, a Chinese native and resident of San Jose, California, was arrested and charged with theft of trade secrets. He reportedly transferred over 3,600 files from the company he worked for to his personal storage devices in an attempt to aid the PRC. Some of these files reportedly contained information on sensors designed for nuclear missile detection as well as other sensitive technologies.
- [March 6, 2024](#): Linwei Ding, a Chinese national residing in California, was charged in an indictment with four counts of theft of trade secrets,⁸ in connection with, a plot to steal artificial intelligence information from Google LLC.
- [March 25, 2024](#): Seven Chinese nationals were charged in New York amidst an indictment with conspiracy to commit computer intrusions and conspiracy to commit wire fraud during their involvement in a PRC-based hacking group. The group targeted U.S. and foreign critics, politicians, and businesses for 14 years.
- [April 25, 2024](#): Two PRC nationals, Han LI and Lin CHEN, were indicted in the Northern District of California for conspiracy to illegally export U.S. technology, including a machine used for processing silicon wafer microchips, to prohibited entities in the PRC. Chen was arrested in Chicago, while Li is believed to be in China.
- [May 24, 2024](#): Former CIA officer, Alexander Yuk Ching Ma, of Honolulu, pled guilty to conducting espionage on behalf of the Chinese government through providing national defense information to the PRC's Shanghai State Security Bureau. [On September 11](#), he was sentenced to 10 years in prison for conspiracy to commit espionage.
- [June 13, 2024](#): Klaus Pflugbeil, a Canadian and German national and resident of the PRC, pleaded guilty in New York, to conspiring to send trade secrets that belonged to a U.S. based electric vehicle company. Pflugbeil used the secrets to build another business that marketed to replace the company in which he stole trade secrets from.
- [July 25, 2024](#): In California, John Chen and Lin Feng, both of the PRC, pleaded guilty to acting as illegal agents of the PRC and bribery of an IRS agent.
- [July 24, 2024](#): Ping Li, of Florida, was charged in an indictment with conspiracy to act as an agent for the PRC and acting as a foreign agent on behalf of the PRC. Li was reportedly a "cooperative contact" for the PRC's Ministry of State Security while Li worked for a major U.S. telecommunications company.

⁸ In general, the theft of trade secrets means: (1) whoever knowingly performs targeting or acquisition of trade secrets or intends to convert a trade secret to (2) knowingly benefit anyone other than then owner. Commonly referred to as industrial espionage. 18 U.S.C. § 1832.

- [August 6, 2024](#): Shujun Wang, a Queens resident, indicted in New York, was convicted on 4 counts charged in an indictment including acting and conspiring to act as a foreign agent of the PRC. Wang helped start a pro-democracy organization that opposed the communist regime in China in order to get close to prominent activists seeking change in the PRC. His 4 co-defendants, officials in the Ministry of State Security, remain at large.
- [August 13, 2024](#): Korbein SCHULTZ, a U.S. Army intelligence analyst, pleaded guilty to multiple charges in the Middle District of Tennessee, including conspiracy to obtain and disclose national defense information and bribery of a public official. Schultz sold sensitive military information to a foreign national suspected of having ties to the PRC government. The FBI and U.S. Army Counterintelligence Command are investigating the matter.
- [August 21, 2024](#): Yuanjun TANG, a naturalized U.S. citizen and resident of Queens, New York, was charged with acting as an unregistered agent of the PRC and making false statements to the FBI. Tang, a former PRC dissident, allegedly acted at the direction of the MSS to report on individuals and groups considered by Beijing to be adverse to PRC interests.
- [September 3, 2024](#): Linda SUN and her husband Chris HU were indicted for violating the Foreign Agents Registration Act and conspiracy to commit money laundering, allegedly acting on behalf of PRC government. While in a senior role in New York State government, Sun is accused of blocking access for Taiwanese representatives and facilitating unauthorized visits for PRC officials. The couple allegedly laundered millions for personal gain, including luxury purchases. They were arraigned in federal court in Brooklyn, New York.
- [September 16, 2024](#): SONG Wu, a PRC national and engineer employed by Aviation Industry Corporation of China—a state-owned conglomerate, was indicted in the Northern District of Georgia for wire fraud and aggravated identity theft related to a scheme to illegally obtain proprietary software and source code from NASA and other U.S. entities. Song allegedly conducted a multi-year spear phishing campaign to impersonate U.S. researchers, targeting government and university personnel to solicit restricted aerospace software for potential military applications in the PRC.
- [September 16, 2024](#): Jia WEI, a PRC national and member of the PRC's People's Liberation Army (PLA) member, was indicted in the Northern District of Illinois for unlawfully accessing the computer network of a U.S. communications company to steal proprietary information for entities in the PRC. Wei allegedly accessed the U.S. company's network shortly after it filed a civil lawsuit against a PRC competitor for theft of trade secrets, stealing documents related to both civilian and military communication devices. The six-count indictment charges Wei with wire fraud, conspiracy to commit computer intrusions, computer intrusions, and aggravated identity theft.
- [October 1, 2024](#): Zhekai Xu, Renxiang Guan, Haoming Zhu, Jingzhe Tao, and Yi Liang, PRC nationals, were indicted in the Eastern District of Michigan for allegedly making false statements and conspiring to delete photos from their phones. According to reports,

all five PRC nationals graduated from the University of Michigan last year. These PRC nationals were enrolled in a joint program between the University of Michigan and Shanghai Jiao Tong University in China.

2023

- [January 19, 2023](#): Nickie Mali LUM DAVIS, of Honolulu, Hawaii, a U.S. citizen and businesswoman, was sentenced to two years in prison for facilitating an unregistered lobbying campaign for the benefit of the Malaysian and PRC governments in exchange for about \$3 million dollars. Regarding the PRC, Lum Davis and three co-conspirators attempted to facilitate the repatriation of a PRC dissident living in the United States by lobbying public officials.
- [January 3, 2023](#): Xiaoqing Zheng, of New York, was sentenced to 24 months in prison for conspiring to steal General Electric (GE) trade secrets in order to benefit the PRC.
- [January 25, 2023](#): A jury in the Northern District of Illinois sentenced, Ji Chaoqun, a Chinese national, to eight years in prison for acting illegally as an agent of the PRC in the U.S. Evidence showed that Chaoqun worked at the direction of high-level intelligence officers in the Ministry of State Security for the PRC with tasks related to recruiting scientists and engineers working in America in order to obtain access to advanced aerospace and satellite technologies being developed by companies within the U.S.
- [April 26, 2023](#): Prakazrel “Pras” MICHEL, of Coconut Creek, Florida, was convicted for conspiring with PRC officials, including the Vice Minister of Public Security, to illegally lobby the U.S. government to repatriate a PRC national. Additionally, Michel worked with Malaysian businessman Jho Low to influence U.S. officials to drop the 1MDB embezzlement investigation on behalf of the Malaysian government. He also illegally funneled millions of dollars from Low into the 2012 U.S. presidential election. Michel’s conviction is related to that of Nickie Mali Lum Davis.
- [April 26, 2023](#): Dr. Charles Lieber, the former chair of the Harvard University Chemistry and Chemical Biology Department, in Massachusetts, was sentenced in federal court to time served in prison; two years of supervised release with six months of home confinement; a fine of \$50,000; and \$33,600 in restitution to the IRS. Unbeknownst to his employer, Dr. Lieber became a “strategic scientist” at the Wuhan University of Technology and was also a participant in China’s Thousand Talents Plan. This occurred while he accepted more than \$15,000,000 in grant funding from the National Institutes of Health and Department of Defense.
- [April 17, 2023](#): Approximately 40 officers of China’s Ministry of Public Security were charged in New York with an indictment amidst various crimes in relation to a transnational repression scheme which targeted PRC dissidents in the United States. The agents also reportedly attempted to recruit U.S. persons to act as agents on behalf of the PRC.
- [April 17, 2023](#): Lu Jianwang, 61, of the Bronx, and Chen Jinping, 59, of Manhattan, were arrested and charged with conspiring to act as agents of the PRC and obstructing justice by destroying evidence of their communications with a PRC Ministry of Public Security

(MPS) official. The two set up and operated an overseas clandestine police station in Manhattan which reported to the Fuzhou branch of the MPS.

- [May 16, 2023](#): Liming Li, of Rancho Cucamonga, was arrested and charged with theft of trade secrets. He allegedly stole trade secrets focused on sensitive technologies from his Southern California based employers and planned to set up a competing company in the PRC.
- [May 16, 2023](#): Weibao WANG, a former Apple employee, was indicted in the Northern District of California for stealing trade secrets related to Apple's autonomous systems technology while secretly working for a Chinese company developing self-driving cars. After downloading sensitive information, Wang attempted to flee to China following an FBI search of his home. He faces up to 10 years in prison for each count of theft or attempted theft of trade secrets.
- [May 15, 2023](#): Litang Liang, of Massachusetts, was indicted on one count of acting as a foreign agent and one count of conspiring to act as a foreign agent on behalf of the PRC. Liang allegedly reported to PRC officials on pro-democracy protests in the United States.
- [June 20, 2023](#): A federal jury in New York convicted three individuals of interstate stalking and two of the defendants for acting or conspiring to act on behalf of the People's Republic of China. The arrests were in connection with Operation Fox Hunt, a PRC campaign to harass, stalk, and coerce certain individuals living in the U.S. to return to the PRC.
- [July 10, 2023](#): Gal LUFT, a dual U.S.-Israeli citizen and co-director of a Maryland-based think tank, was indicted for working as an unregistered agent of the PRC and advancing its interests in the United States. Luft allegedly recruited a former U.S. official to support PRC-favorable policies, brokered illicit arms deals involving Chinese entities, and facilitated the sale of Iranian oil to the PRC while evading U.S. sanctions.
- [August 3, 2023](#): Jinchao Wei, a U.S. Navy sailor in California, was arrested at Naval Base San Diego on espionage charges with conspiracy to send national defense information to an intelligence agent of the PRC.
- [October 6, 2023](#): Joseph Daniel SCHMIDT, a former U.S. Army Sergeant, whose last duty post was Joint Base Lewis-McChord in Western Washington was indicted for attempting to deliver national defense information and for unlawful retention of national defense information. Schmidt allegedly tried to provide classified military information to PRC intelligence services after leaving the military in January 2020. According to the indictment, Schmidt retained a device capable of accessing secure military computer networks and offered it to PRC authorities to aid their efforts in compromising U.S. defense systems.
- [December 6, 2023](#): Hans Maria DE GEETERE, a Belgian national, was charged with orchestrating the illegal export of sensitive U.S. military technology to the PRC and the Russian Federation. He faces charges for smuggling electronic components used in missiles and military radar, as well as attempting to export accelerometers for aerospace

and military systems to the PRC. The case was coordinated through the Disruptive Technology Strike Force co-led by the DOJ and Department of Commerce.

2022

- [February 7, 2022](#): A federal indictment alleges China based Hytera Communications Corp. recruited and hired Chicago-based Motorola Solutions employees and directed them to take trade secret information from Motorola without authorization.
- [March 23, 2022](#): Zhongsan Liu, of New Jersey, was convicted of participating in a scheme to defraud the United States by obstructing the legal processes of the Department of State and Department of Homeland Security and committing visa fraud. Liu attempted to obtain fraudulent research scholar visas for employees of the government of the PRC.
- [April 7, 2022](#): Xiang Haitao, a former resident of Missouri, was sentenced to 29 months in prison for conspiring to commit economic espionage on behalf of the PRC when he conspired to steal a trade secret from the Climate Corporation.
- [May 9, 2022](#): Dr. Xiaorong You, aka Shannon You, 59, of Lansing, Michigan was sentenced to serve 168 months in prison for conspiracy to commit trade secret theft, conspiracy to commit economic espionage, possession of stolen trade secrets, economic espionage, and wire fraud. You used trade secrets to establish a company in China and received millions in funding from the Chinese government.
- [May 18, 2022](#): One U.S. citizen and four Chinese nationals were charged with spying on dissidents, human rights leaders, and pro-democracy activists. Wang Shu, of New York, created a pro-democracy organization but acted as a covert agent in his own organization spying on those opposed to the Chinese government. The four Chinese nationals involved are members of the Ministry of State Security by the names of Feng He, Jie Ji, Ming Li, and Keqing Lu.
- [May 19, 2022](#): Chenyan Wu and Lianchun Chen, a married couple and research scientists for an American pharmaceutical company in California, pleaded guilty to criminal charges that stemmed from their efforts to gather mRNA research from the company they worked for in order to aid the husband's company in China.
- [June 16, 2022](#): Simon Saw-Teong Ang of Arkansas, a former University of Arkansas professor, was sentenced to 12 months and 1 day in prison for making a false statement to the FBI about the existence of patents for his inventions in the PRC.
- [July 7, 2022](#): Five men were indicted in New York for various crimes involving a transnational repression scheme to silence critics of the PRC residing in the United States.
- [September 20, 2022](#): Former Broadcom engineer, Peter Kisang Kim of California, was sentenced to 8 months in prison for trade secret theft. After leaving Broadcom, he used trade secrets in a new role in a PRC based tech startup.
- [November 7, 2022](#): Former U.S. Army pilot Shapour Moinian, of California, was sentenced to 20 months in prison for acting as an agent of the government of the PRC. He accepted cash payments from Chinese representatives for providing defense aviation related information.
- [November 9, 2023](#): The DOJ indicted three individuals (Phil Pascoe, 60, of Floyds Knobs, Indiana; Monica Pascoe, 45, of Floyds Knobs, Indiana; Scott Tubbs, 59, of Georgetown, Kentucky) and Quadrant Magnetics LLC for wire fraud and violating the

Arms Export Control Act. The DOJ also indicted these individuals and this company for participating in a scheme to smuggle controlled, defense-related data to the PRC and to unlawfully provide the Department of Defense with PRC-origin rare earth materials for aviation and military systems.

- [November 16, 2022](#): Yanjun Xu, Deputy Division Director of the Sixth Bureau of the Jiangsu Province Ministry of State Security, was sentenced in Ohio to 20 years in prison for conspiring to and attempting to commit economic espionage and theft of trade secrets. He is the first Chinese intelligence officer to be extradited to the United States.

2021

- [February 3, 2021](#): Lin Yang, a former University of Florida professor, was indicted in Florida for fraudulently obtaining \$1.75 million in grant money from the NIH by concealing his involvement with and support from the Chinese government. Additionally, it was found that Yang applied for and was accepted into China's Thousand Talents Program.
- [February 19, 2021](#): Chen Song, a former Stanford University researcher was charged in California, in an indictment with visa fraud, obstruction of justice, destruction of documents, and false statements in connection with a scheme to conceal and lie about her status as a member of the PRC's military forces while in the United States.
- [February 1, 2021](#): Li Chen, of Dublin, Ohio, was sentenced to 30 months in prison for conspiring with her husband to steal exosome related trade secrets in order to sell them to China. Her husband, Yu Zhou, is noted below.
- [February 26, 2021](#): Chi Lung Winsman Ng, a Hong Kong businessman, was indicted for conspiring to steal General Electric's (GE) trade secrets involving extremely valuable MOSFET technology.
- [April 20, 2021](#): Yu Zhou, of Ohio, was sentenced to 33 months in prison for conspiring to steal exosome related trade secrets from Nationwide Children's Hospital's Research Institute in order to sell them to China.
- [April 21, 2021](#): Mingqing Xiao, of Illinois, a mathematics professor at Southern Illinois University, was charged in an indictment with two counts of wire fraud and one count of making a false statement. Xiao fraudulently obtained grant money from the National Science Foundation by concealing support he was receiving from the Chinese government and a Chinese university.
- [May 14, 2021](#): Song Guo Zheng, a former professor at Ohio State University and Pennsylvania State University, was sentenced to 37 months in prison for lying to federal authorities in order to use \$4.1 million in grants from the NIH. He used this to develop China's expertise in the areas of rheumatology and immunology in another case involving China's Thousand Talents Program.
- [June 16, 2021](#): Meyya Meyyappan, a former senior NASA scientist was sentenced in New York to time in prison for making false statements to the FBI about his involvement in China's Thousand Talents Program.
- [July 19, 2021](#): Four Chinese hackers were charged in California in an indictment that alleges they were apart of campaign to hack U.S. companies between 2011-2018 focusing on the theft of intellectual property.

- [July 22, 2021](#): Yi-Chi Shih, of California, was sentenced to 63 months in federal prison on multiple charges stemming from a plot to illegally obtain semiconductor chips with military uses and export them to China.
- [July 16, 2021](#): Ge Songtao, of the PRC, was sentenced by the Middle District of Florida to 3 years and 6 months in prison for conspiring to export maritime raiding craft and engines to China fraudulently. These vessels and engines are used by the U.S. military and no comparable engine is manufactured in China.
- [September 9, 2021](#): Shuren Qin was sentenced in Massachusetts for illegally procuring and exporting U.S. goods to Northwestern Polytechnical University (NWPU), a Chinese military university that is heavily involved in military research and the PLA. He reportedly exported hydrophones with military applications in anti-submarine warfare.
- [October 25, 2021](#): Former Air War College professor, Xiaoming Zhang, pled guilty in Alabama to making false statements about his relationship with a Chinese government official.
- [December 21, 2021](#): Former U.S. Navy sailor, Ye Sang “Ivy” Wang, was sentenced in California to 30 months in prison for conspiring with her husband to illegally export sensitive military equipment to China for profit.