Survey of Chinese-linked Espionage in the United States Since 2000

This survey lists 152 publicly reported instances of Chinese espionage directed at the United States since 2000.[1] It does not include espionage against other countries, U.S. firms or persons located in China, nor an additional 50 cases involving attempts to smuggle munitions or controlled technologies from the U.S. to China. We also did not include more than 1200 cases of intellectual property litigation brought by U.S. companies against Chinese entities in either the U.S. or Chinese legal systems.[1]

For those cases where we could identify actor and intent, we found:

- 45% of actors were Chinese military or government employees.
- 30% were private Chinese citizens.
- 33% involved non-Chinese actors (usually U.S. persons recruited by Chinese officials)
- 38% of incidents sought to acquire military technology.
- 48% of incidents sought to acquire commercial technologies.
- 14% of incidents sought to acquire information on U.S. civilian agencies or politicians.

These reported incidents are derived from open source material. The sources are endnoted. The list may not reflect the full number of incidents and may not be complete. Of the 152 incidents, the decadal breakdown is:

- 2000-2009: 26%
- 2010-2020: 74%

This could reflect an increase in the number of incidents after 2009, but it may also reflect variances in the public reporting of espionage cases, as greater attention was paid to the problem and the U.S. government reportedly became less resultant to publicly identify China as the perpetrator after 2007.

The list of individual incidents follows below.

May 2001: Beginning in January 2000, Hai Lin, Kai Xu, and Yong-Qing Cheng formed a joint venture with the Datang Telecom Technology Company of Beijing to steal trade secrets from Lucent.[2]

2003: Chinese hackers exfiltrated national security information from Naval Air Weapons Station China Lake, including nuclear weapons test and design data, and stealth aircraft data.

[1] We would like to thank Evan Burke, Matthew Serrone, Khristal Thomas, Arthur Nelson, and Ian Haimowitz for their contributions to this timeline.

April 2003: Katrina M. Leung was arrested for convincing an FBI agent to share classified information, which she passed on to China, over a ten-year period.[3]

February 2004: Ronald N. Montaperto, a former DIA intelligence analyst, was arrested for providing Chinese military attaches with Secret and Top-Secret information.[4]

July 2004: Yan Ming Shan, a Chinese employee of a U.S. software firm that develops land sensing technology for oil companies, gained unauthorized access to the company's computer system and attempted to bring sensitive technology back to China.[5]

June 2005: Noshir Gowadia, an American citizen, took six trips to China between 2003-2005 to assist with its cruise missile system by developing a stealthy exhaust nozzle and was paid at least $110,000 by China. He provided them with designs for a low-signature cruise missile exhaust system.[6]

October 2005: Chi Mak and other Chinese intelligence operatives collected technical information about the Navy's current and future warship technologies. Chi intended to export the information to China.[7]

November 2005: Moo Ko-Suen was a representative for an American aerospace firm for 10 years in Taiwan, during which time he acted as an agent for the Chinese government and tried to buy sophisticated military parts and weapons, including an F-16 fighter jet engine and cruise missiles, for China.[8]

2005: Chinese hackers infiltrated U.S. Department of Defense networks in an operation known as "Titan Rain." They targeted U.S. defense contractors, Army Information Systems Engineering Command; the Defense Information Systems Agency; the Naval Ocean Systems Center; and, the U.S. Army Space and Strategic Defense installation.[9]

April 2006: Chinese hackers infiltrated NASA networks managed by Lockheed Martin and Boeing and exfiltrated information about the Space Shuttle Discovery program.[10]

May 2006: Shanshan Du stole trade secret information from General Motors for the benefit of a Chinese competitor, Chery Automobile.[11]

June 2006: Lan Lee and Yufei Ge conspired to steal trade secrets related to computer chip design and development from NetLogics Microsystems and TSMC.[12]

July 2006: Chinese hackers infiltrated the U.S. State Department's unclassified network and stole sensitive information and passwords.[13]

August 2006: Chinese hackers infiltrated the Department of Defense's non-classified NIPRNet, downloading 10 to 20 terabytes of data.[14]

December 2006: Xiaodong Sheldon Meng, a resident of Beijing and Cupertino California, stole military IP and trade secrets from his former employer, the silicon valley firm Quantum3D.[15]

December 2006: Fei Ye and Ming Zhong stole trade secrets from two American technology firms to benefit China. They intended to utilize the secrets to build microprocessors for their company, Supervisor Inc. which would share any profits made on the sale of chips to the City of Hangzhou and the Province of Zhejiang in China.[16]

December 2006: Xiang Dong Yu stole trade secret information worth $50-100 million from Ford Motor Company for the benefit of Beijing Automotive Company.[17]

December 2006: Chinese hackers infiltrated the U.S. Naval War College[18]

2007: Chinese hackers breached the Pentagon's Joint Strike Fighter project and stole data related to the F-35 fighter jet.[19]

January 2007: The National Defense University discovered Chinese malware in its computer systems.[20]

June 2007: PLA hackers breached a Pentagon computer network serving the Secretary of Defense, forcing the network to be shut down for more than a week.[21]

September 2007: Hackers gained access to the Department of Homeland Security's networks through a contractor and exfiltrated unclassified information to Chinese servers.[22]

December 2007: Chinese hackers successfully stole information from Oak Ridge National Laboratory, Los Alamos National Laboratory, and the National Nuclear Security Administration.[23]

January 2008: Qinggui Zeng stole trade secret information related to the paint industry from an American firm for the benefit of a Chinese firm.[24]

February 2008: The Department of Justice charged Dongfan Chung, a former Boeing engineer, with economic espionage and serving as a foreign agent for China. Prosecutors determined that he had been acting on Chinese orders since at least 1979. He stole Boeing trade secrets relating to the Space Shuttle, the C-17 military transport aircraft and the Delta IV rocket for China.[25]

February 2008: Tai Shen Kuo, a U.S. citizen, was arrested for providing China with classified information between March 2007 to February 2008. Kuo obtained the information from a Pentagon weapons system policy analyst, Gregg Bergersen.[26]

March 2008: Hanjuan Jin attempted to leave the country with 1000+ electronic and paper copies of proprietary information related to Motorola's interstate communication feature.[27]

May 2008: Chinese officials inserted spyware onto the laptop of U.S. Secretary of Commerce Carlos Gutierrez during a trade mission..[28]

September 2008: Anne Lockwood and Fuping Liu stole trade secret information from

Metaldyne to benefit a Chinese competitor, Huafu.[29]

November 2008: Chinese hackers infiltrated the computer networks of three major oil companies and stole trade secret information.[30]

November 2008: Chinese hackers infiltrated the networks of Barack Obama and John McCain's presidential campaigns and exfiltrated information about future policy agendas.[31]

November 2008: Chinese hackers infiltrated the computer network of the White House and obtained emails between senior government officials.[32]

March 2009: David Yen Lee, a technical director with Valspar Corp, illegally downloaded Valspar trade secrets with the intent of delivering them to Nippon Paint in Shanghai, where he had accepted a vice president position.[33]

March 2009: Chinese hackers infiltrated Coca-Cola Co. computer networks and stole trade secret information, including information related to the attempted $2.4 billion acquisition of Huiyuan Juice Group.[34]

March 2009: Chinese hackers stole information from the Office of Senator Bill Nelson in Florida.[35]

April 2009: Yan Zhu, along with unidentified co-conspirators, planned to steal trade secrets relating to computer systems and software with environmental applications from his U.S. employer.[36]

October 2009: Hong Meng accepted employment as a faculty member at Peking University, and thereafter began soliciting funding to commercialize his research from Dupont on Organic Light-Emitting Diodes. He shared trade secret chemical processes, including those related to OLEDs, with PKU.[37]

November 2009: Janice Capener, a Chinese national, stole trade secret information from Orbit Irrigation for the benefit of a competing Chinese firm.[38]

January 2010: Beginning in 2009, China carried out a series of cyberattacks to steal trade secret information from dozens of U.S. companies including Google, Yahoo, Adobe, Dow Chemical, and Morgan Stanley.[39]

2010: The PLA infiltrated the computer network of a Civilian Reserve Air Fleet (CRAF) contractor in which documents, flight details, credentials and passwords for encrypted email were stolen.[40]

May 2010: Glenn Shriver attempted to gain access to classified national defense information on behalf of Chinese intelligence officers.[41]

May 2010: Chinese hackers breached the computer network of the U.S. Chamber of Commerce and stole information related to U.S. industries.[42]

August 2010: Kexue Huang, a Chinese research scientist, stole trade secret information related to organic pesticides for the benefit of a Chinese firm.[43]
November 2010: Zhiqiang Zhang allegedly stole trade secret information from SiRF for the benefit of a competing Chinese firm.[44]

January 2011: A Chinese company, Pangang Group, and Walter Liew attempted to steal trade secret information related to TiO_2 technology from DuPont.[45]

February 2011: Wen Chyu Liu, a research scientist, conspired to steal trade secret information from Dow for the benefit of Chinese firms.[46]

March 2011: Sinovel, a Chinese company, stole trade secret information related to source code and designs of superconductors from AMSC.[47]

March 2011: Chinese hackers breached the RSA Security division of the EMC Corporation to steal information related to encryption software, compromising RSA SecureID tokens. The stolen information was used in subsequent attacks carried out by China.[48]

April 2011: Chinese hackers engaged in a phishing campaign aimed at compromising hundreds of Gmail passwords for accounts of prominent people, including senior U.S. officials. [49]

April 2011: Chinese hackers attempted to steal technical data from the computer systems of Oak Ridge National Laboratory.[50]

June 2011: Beginning in 2010, Chunlai Yang conspired to steal trade secret information related to the source code of the OS for the Globex electronic trading platform for the benefit of a Chinese firm.[51]

August 2011: Chinese hackers engaged in a series of cyber-attacks against 72 entities, including multiple U.S. government networks.[52]

October 2011: Chinese hackers infiltrated at least 48 chemical and defense companies and stole trade secret information and sensitive military information.[53]

November 2011: Chinese hackers interfered with U.S. satellites and stole sensitive data.[54]

February 2012: Chinese hackers stole classified information about the technologies onboard F-35 Joint Strike Fighters.[55]

March 2012: NASA's Inspector General reported that Chinese hackers conducted 13 attacks against NASA computers in 2011. In one attack, intruders stole 150 user credentials that could be used to gain unauthorized access to NASA systems. Another attack at the Jet Propulsion Laboratory allowed intruders to gain full access to key JPL systems and sensitive user accounts.[56]

June 2012: DHS reported that between December 2011 and June 2012, Chinese hackers

targeted 23 gas pipeline companies and stole information that could be used for sabotage purposes.[57]

June 2012: P.L.A. Unit 61398 attacked Digital Bond, a SCADA security company with a spear phishing attack.[58]

August 2012: Jerry Lee, a former CIA agent, attempted to provide China with classified information about CIA activities within China.[59]

September 2012: Employees of a semiconductor chip equipment manufacturer stole trade secrets related to high-volume manufacturing of semiconductor wafers used in electronic devices for the benefit of a competing Chinese firm.[60]

September 2012: Sixing Liu, a Chinese national, stole technical data related to defense items and conspired to give the information to China.[61]

September 2012: Ji Li Huang and Xiao Guang Qi attempted to steal trade secret information related to cellular glass installation for the benefit of a competing Chinese firm.[62]

November 2012: Wenfeng Lu, a Chinese national, stole trade secret information for medical devices from American medical equipment manufacturers for the benefit a Chinese firm.[63]

January 2013: The FBI warned Senator Dianne Feinstein's office that one of her San Francisco-based drivers was a Chinese intelligence asset.[64]

January 2013: A Defense Science Board report found that Chinese hackers stole U.S. weapons systems designs including for the PAC-3, THAAD, Aegis, F/A-18 fighter jet, V-22 Osprey, Black Hawk, and Littoral Combat Ship.[65]

January 2013: The New York Times, Wall Street Journal, Washington Post, and Bloomberg News experienced persistent cyberattacks, presumed to originate in China.[66]

February 2013: Security researchers revealed that PLA Unit 61398 had hacked 115 U.S.-victims since 2006, including organizations in the IT, aerospace, and telecommunicatinos sectors, among others.[67]

March 2013: Beginning in 2012, Chinese hackers targeted civilian and military maritime operations within the South China Sea, in addition to U.S. companies involved in maritime satellite systems, aerospace companies and defense contractors.[68]

May 2013: Chinese hackers compromised the U.S. Department of Labor and at least nine other agencies, including the Agency for International Development and the Army Corps of Engineers' National Inventory of Dams.[69]

June 2013: PLA hackers infiltrated the computer networks of the U.S. Transportation Command and stole sensitive military information.[70]

July 2013: Tung Pham stole trade secrets from a solar technology company for the benefit of a competing Chinese firm.[71]

September 2013: Chinese hackers targeted three U.S. organizations, including a large American oil and gas corporation.[72]

September 2013: Chinese hackers used malware, known as 'Sykipot', to target entities in the U.S. defense industrial base and companies in key industries such as telecommunications, computer hardware, government contractors, and aerospace.[73]

October 2013: Chinese hackers targeted a U.S. based think tank.[74]

December 2013: Six Chinese nationals conspired to steal trade secret information related to seeds from Dupont, Monsanto, and LG seeds for the benefit of Beijing Dabeinong Technology Group, a competing Chinese firm.[75]

December 2013: Weiqiang Zhang stole trade secret information related to rice seeds from an American agricultural firm for the benefit of a Chinese firm.[76]

February 2014: Amin Yu stole systems and components for marine submersible vehicles from U.S. manufacturers for the benefit of a state-owned entity in China.[77]

May 2014: Chinese military hackers targeted six American companies in the power, metals, and solar production industries and stole trade secret information.[78] The U.S. Department of Justice indicted them and identified them as members of the People's Liberation Army Unit 61398.

June 2014: CrowdStrike reported that Unit 61398 had targeted U.S. corporations in the satellite industry.[79]

June 2014: Jun Xie allegedly stole trade secret information from GE Healthcare to benefit a competing entity in China.[80]

August 2014: Community Health Systems disclosed that suspected Chinese hackers infiltrated its network and stole personal information from 4.5 million patients.[81]

August 2014: Su Bin, a Chinese national, worked with co-conspirators in China to infiltrate Boeing's computer networks to gain access to confidential access about the C-17, the F-22, and the F-35.[82]

August 2014: Chinese hackers infiltrated the U.S. Investigations Services. This was one of the first steps in the 2015 OPM hack.[83]

September 2014: Chinese company Huawei repeatedly attempted to steal trade secret information about robotics designs from T-Mobile.[84]

September 2014: Benjamin Bishop was arrested for passing classified information between May 2012 – December 2012 to a Chinese national he was romantically involved with.[85]

November 2014: Chinese hackers breached the U.S. Postal Service computer networks and exfiltrated data of approximately 800,000 employees.[86]

November 2014: Yu Long worked at URTC from 2008-2014, but was recruited by the state-run Shenyang Institute of Automation in 2014. Upon departure Long stole confidential IP, trade secrets, and export-controlled technology to give to SIA for the benefit of China.[87]

February 2015: Xudong Yao stole trade secret information relating to locomotives for the benefit of a Chinese firm.[88]

January 2015: Chinese hackers, including Fujie Wang, infiltrated Anthem Inc., a health insurer company, and stole data concerning approximately 78.8 million people from Anthem's computer networks.[89]

March 2015: Canadian researchers say Chinese hackers attacked U.S. hosting site GitHub. GitHub said the attack involve a wide combination of attack vectors and used new techniques to involve unsuspecting web users in the flood of traffic to the site. According to the researchers, the attack targeted pages for two GitHub users – GreatFire and The New York Times' Chinese mirror site – both of which circumvent China's firewall. [90]

April 2015: The Office of Personnel Management discovered that China had infiltrated its networks and stolen the personal information of federal employees, including security clearance information.[91]

May 2015: Xiwen Huang, a Chinese businessman, stole confidential and trade secret information – including intellectual property – from an unnamed government research facility related to military vehicle fuel cells, for the benefit of China.[92]

May 2015: Chinese intelligence officers infiltrated networks and exfiltrated trade secret information about turbofan engines from U.S. and European aerospace firms over the course of five years.[93]

May 2015: Beginning in 2014, Thomas Rukavina stole and passed on trade secret information from PPG to a competing Chinese firm.[94]

May 2015: Chinese nationals Wei Pang and Hao Zhang stole trade secrets related to the development of thin-film bulk acoustic resonator (FBAR) technology for the benefit of China.[95]

May 2015: Chinese hackers exfiltrated significant amounts of customer data from United Airlines.[96]

September 2015: Robert O'Rourke allegedly illegally downloaded data from his employer, an American manufacturer of cast-iron products. O'Rourke had accepted a similar position with a

rival firm in China and was planning to use the stolen IP to improve the competitiveness of his new firm's products.[97]

December 2015: Chinese National Xu Jiaqiang conspired to steal source code from an unnamed U.S. company where he worked as software developer. Xu intended to transfer the stolen code to benefit China's National Health and Family Planning Commission.[98]

January 2016: Tao Li and co-defendants Yu Xue & Yan Mei engaged in conspiracy to steal trade secrets from GlaxoSmithKline (GSK) for the benefit of a Chinese firm.[99]

March 2016: Kun Shan Chun, a naturalized U.S. citizen, was sentenced to 24 months in prison for acting as an agent of China. Chun, an FBI employee with a top-secret clearance, provided a Chinese government official with sensitive, nonpublic information about FBI surveillance methods, internal organization, and identify and travel patterns of an FBI special agent.[100]

April 2016: Szuhsiung Ho, an American nuclear engineer employed as a consultant by CGNPC, provided engineers and experts to assist CGNPC in developing nuclear material and reactors between 1997 and 2016 without authorization from DOE.[101]

March 2017: A State Department employee with TS clearance provided copies of internal Department of State documents to Chinese intelligence officers.[102]

April 2017: Chinese hackers targeted a U.S. think tank.[103]

May 2017: Beginning in 2011, Hackers from the internet security firm Boyusec compromised the networks of three companies over a multi-year period and gained access to confidential documents and data, including sensitive internal communications, usernames and passwords, and business and commercial information.[104]

June 2017: U.S. citizen Shan Shi and Chinese national Gang Liu worked on behalf of Chinese company CBM-Future New Material Science and Technology Co. Ltd. (CBMF) to steal trade secrets related to the development of syntactic foam from an unnamed global engineering firm.[105]

June 2017: Kevin Patrick Mallory, a former CIA officer, transferred classified documents to an agent of China's intelligence services.[106]

August 2017: Dong Liu attempted to obtain trade secret information from Medrobotics Corporation for China.[107]

September 2017: China allegedly inserted malware into a widely used PC management tool. The malware targeted at least 20 major international technology firms.[108]

October 2017: China allegedly carried out a cyberattack against a U.S. think tank and law firm, both of which were associated with fugitive Chinese tycoon Guo Wengui.[109]

October 2017: Jerry Jindong Xu sought to help Chinese investors build a sodium cyanide plant to compete with Chemours by stealing pricing information, passwords for spreadsheets, confidential documents, and plant system diagrams from Chemours while he was employed there.[110]

January 2018: Yi-Chi Shih and Kiet Ahn Mai stole trade secret information from Monolithic Microwave Integrated Circuit (MMIC) technology for the benefit of Chengdu GaStone Technology Company (CGTC), a competing Chinese firm.[111]

January 2018: Chinese hackers infiltrated a U.S. Navy contractor working for the Naval Undersea Warfare Center. 614 gigabytes of material related to a supersonic anti-ship missile for use on U.S. submarines were taken, along with submarine radio room information related to cryptographic systems and the Navy submarine development unit's electronic warfare library.[112]

April 2018: Yanjun Xu, an MSS operative, attempted to recruit experts employed by leading American aviation companies to China, often under the guise of giving a presentation at a university.[113]

April 2018: A cyber espionage campaign originating in China collected data from satellite, telecom, and defense organizations in the United States and Southeast Asia.[114]

June 2018: Ron Rockwell Hansen, a former DIA officer, attempted to transmit national defense information to China.[115]

July 2018: Xiaqing Zhang conspired to steal trade secret information from General Electric for the benefit of China.[116]

July 2018: Xiaolang Zhang was arrested for stealing trade secret information about the circuit board of Apple's self-driving car initiative. The case is still active as of August 2019.[117]

September 2018: Chinese hackers breached the systems of the Starwood hotel chain in 2014. It is estimated that the personal information of up to 500 million people was stolen.[118]

September 2018: Ji Chaoqun, a Chinese citizen residing in Chicago, worked at the behest of the Jiangsu Province Ministry of State Security (JSSD) to get biographical information on eight Chinese nationals working as engineers and scientists in the United States that the JSSD had targeted for recruitment. Some worked for U.S. defense contractors.[119]

November 2018: Chen Zhengkun, He Jianting, and Wang Yungming stole Micron trade secrets related to dynamic random-access memory technology (DRAM) for the benefit of China.[120]

November 2018: Beginning in March 2017, U.S. citizen Xiaorong You and Chinese national Liu Xiangchen conspired to steal trade secrets worth more than $100 million related to the development of BPA-free coatings. You stole trade secrets from the two American companies that employed her and provided them to Liu, whose company used them to create products that would compete with the two American companies in question.[121]

December 2018: A Chinese national, Hongjin Tan, was arrested for stealing trade secret information from an American petroleum company, Phillips 66, and conspiring to use to benefit a Chinese firm.[122]

December 2018: Chinese hackers stole IP and confidential business and technological information from managed service providers – companies that manage IT infrastructure for other businesses and governments.[123]

December 2018: Chinese hackers stole hundreds of gigabytes of data from computers of more than 45 technology companies and U.S. government agencies. The defendants also stole names, SSNs, DOBs, salary info, phone numbers, and email addresses of more than 100,000 U.S. Navy personnel.[124]

January 2019: A Chinese national, Jizhong Chen, stole trade secret information about autonomous vehicles from Apple to benefit a competing Chinese firm**.**[125]

March 2019: Beginning in April 2017, Chinese hackers stole research from universities about maritime technology being developed for military use.[126]

March 2019: Chinese hackers targeted Israeli defense firms that had connections to the U.S. military.[127]

April 2019: Chinese hackers stole General Electric's trade secrets concerning jet engine turbine technologies.[128]

June 2019: Haoyang Yu was arrested in connection with stealing proprietary information from Analog Devices, a U.S. semiconductor company. [129]

June 2019: Since at least 2017, Chinese hackers exfiltrated Call Detail Records (CDRs) from telecommunication companies to track dissidents, officials, and suspected spies.[130]

July 2019: Chinese hackers targeted three U.S. utility companies with a phishing campaign to gain access to computer networks.[131]

August 2019: State-sponsored Chinese hackers conducted a spear-phishing campaign against employees of three major U.S. utility companies.[132]

August 2019: Active since 2012, a previously unidentified Chinese espionage group, APT41, gathered data from firms in telecommunications, healthcare, semiconductor manufacturing, and machine learning. The group was also active in the theft of virtual currencies.[133]

August 2019: Alexander Yuk Ching Ma, a former CIA officer, and his relative were arrested for transmitting Top Secret intelligence to China. Their operation occurred for over a decade, with further attempts to infiltrate the FBI.[134]

September 2019: Two Chinese nationals stole sensitive exosome medical research from the Nationwide Children's Hospital.[135]

September 2019: Zhongsan Liu was arrested for fraudulently gaining J-1 visas for Chinese government officials. Such an incursion was meant to bring in facilitators of "talent-recruitment programs," a known Chinese espionage tactic.[136] [137]

September 2019: Ron Rockwell Hansen, a former DIA officer, pleaded guilty to facilitating and transmitting Secret military information for the Chinese government.[138]

September 2019: Xuehua "Edward" Peng was charged for acting as an illegal foreign agent for his delivering of classified information to the Chinese Ministry of State Security. [139]

November 2019: Jerry Chun Shing Lee, a former CIA officer, was sentenced for providing classified information to Chinese intelligence officers.[140]

January 2020: A Harvard University Professor, Dr. Charles Lieber, and two Chinese nationals, Yanqing Ye and Zaosong Zheng, were indicted for attempted theft of biological research. Dr. Lieber was a participant in the Thousand Talents Plan while actively accepting the National Institutes of Health and Department of Defense funding. Ye, a lieutenant of the PLA, compiled information on U.S. military projects for the CCP. Zheng committed the theft of 21 biological research vials to promote Chinese projects.[141]

June 2020: Hao Zhang, a Chinese national, was convicted under charges of economic espionage and theft of trade secrets from two companies involved semiconductor design and processing.[142]

July 2020: Four Chinese nationals were charged with visa fraud due to their connection with the PLA. Efforts included observing U.S. labs and institutions to replicate research and designs in China.[143]

July 2020: Juan Wei "Dickson" Yeo, was arrested for acting as an illegal agent for the Chinese government. Efforts included creating a fake consulting company to recruit cleared professionals to obtain information for the PRC.[144]

July 2020: Saw-Teong Ang, a University of Arkansas professor, was indicted for wire fraud for his acceptance of U.S contracting funds related to NASA and the Air Force while being employed by Chinese entities.[145]

August 2020: Zhengdong Cheng, a professor at Texas A&M, was charged with wire fraud for concealing his affiliation with Chinese universities and enterprises while accepting a NASA grant. His position allowed him access to sensitive NASA projects. He was a participant of the Thousand Talents Plan. [146]

August 2020: Guan Lei was charged with destruction of evidence during an FBI investigation. Guan is being investigated for transferring sensitive software and other technical data to the PLA and China's National University of Defense Technology. [147]

September 2020: Baimadajie Angwang, an NYPD officer and U.S. Army reservist, was charged as acting as an illegal agent of the PRC. He attempted to gather information on Chinese citizens living in the U.S. and recruit intelligence sources. [148]

June 2015: Media reporting suggested that a Congressman and other American politicians was cultivated by an alleged Chinese spy[149]

October 2020: Lei Gao was charged with conspiring to steal trade secrets from a U.S. oil and gas manufacturer to benefit a Chinse firm[150]

November 2020: Song Guo Zheng, a professor of internal medicine at Ohio State University and Pennsylvania State University, pled guilty to making false statements to federal authorities as part of a scheme to use over $4 million in grants from the NIH to develop China's expertise in rheumatology and immunology through his undisclosed partnership with a Chinese university controlled by the Chinese government.[151]

November 2020: Wei Sun, an electrical engineer with Raytheon, was sentenced to 38 months in federal prison for transporting sensitive missile technology to China on his laptop.[152]

Notes

[1] An initial search of IP litigation identified 1200+ cases of U.S. entities against Chinese entities. The results were based on data listed in the U.S. Public Access to Court Electronic Records (PACER) database, Lex Machina, and annual statistics released by China's Supreme People's Court on judicial enforcement of IPR in China. While the total volume of IP litigation may reflect a concerning trend of Chinese-sponsored intellectual property theft, individual cases do not denote espionage.

[2] https://www.justice.gov/archive/criminal/cybercrime/press-releases/2002/lucentSupIndict.htm

[3] https://evergreen.loyola.edu/khula/www/strategic-intelligence/intel/Leung-DOJ-finalreport.pdf; https://oig.justice.gov/special/s0605/final.pdf

[5] https://www.eastbaytimes.com/2004/12/18/consultant-pleads-guilty-in-tech-theft-2/amp/

[6] https://www.justice.gov/opa/pr/hawaii-man-sentenced-32-years-prison-providing-defense-information-and-services-people-s

[7] https://www.justice.gov/archive/opa/pr/2008/March/08_nsd_229.html

[8] http://www.nbcnews.com/id/12836771/ns/us_news-security/t/taiwanese-man-admits-acting-covert-agent/#.XUSUGm9KjIU

[9] https://www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html

[10] https://www.bloomberg.com/news/articles/2008-11-19/network-security-breaches-plague-nasa

[11] https://www.justice.gov/file/347376/download: https://www.cbsnews.com/news/couple-convicted-of-stealing-gm-trade-secrets

[12] https://www.justice.gov/archive/criminal/cybercrime/press-releases/2006/liIndict.htm

[13] https://www.cbsnews.com/news/state-department-computers-hacked/

[14] https://gcn.com/articles/2006/08/17/red-storm-rising.aspx

[15] https://www.justice.gov/archive/criminal/cybercrime/press-releases/2006/mengCharge.htm

[16] https://www.justice.gov/archive/criminal/cybercrime/press-releases/2006/yePlea.htm

[17] https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2012/03/15/yuPlea.pdf

[18] https://fcw.com/articles/2006/12/04/china-is-suspected-of-hacking-into-navy-site.aspx?sc_lang=en

[19] Dreazen, "Computer Spies Breach Fighter-Jet Project."

[20] https://www.washingtontimes.com/news/2007/jan/12/20070112-123024-8199r/

[21] https://www.ft.com/content/9dba9ba2-5a3b-11dc-9bcd-0000779fd2ac

[22] http://www.cnn.com/2007/US/09/24/homelandsecurity.computers/index.html

[23] http://www.nytimes.com/2007/12/09/us/nationalspecial3/09hack.html

[24] https://www.justice.gov/archive/criminal/cybercrime/press-releases/2008/zengConvict.pdf

[25] http://www.nbcnews.com/id/35300466/ns/us_news-security/t/chinese-born-engineer-gets-years-spying/

[26] https://www.nytimes.com/2008/07/10/washington/10spy.html

[27] https://www.justice.gov/archive/criminal/cybercrime/press-releases/2008/jinIndict

[28] http://www.nbcnews.com/id/24880526/ns/us_news-security/t/did-chinese-hack-cabinet-secretarys-laptop/

[29] https://www.justice.gov/archive/criminal/cybercrime/press-releases/2008/lockwoodPlea.pdf

[30] https://www.csmonitor.com/USA/2010/0125/US-oil-industry-hit-by-cyberattacks-Was-China-involved

[31] http://www.cnn.com/2008/TECH/11/06/campaign.computers.hacked/

[32] https://www.ft.com/content/2931c542-ac35-11dd-bf71-000077b07658

[33] https://www.justice.gov/nsd/files/export_case_list_june_2016_2.pdf/download

[34] https://www.bloomberg.com/news/articles/2012-11-04/coke-hacked-and-doesn-t-tell

[35] https://miamiherald.typepad.com/nakedpolitics/2009/03/nelson-gets-hacked-and-hacked-off.html

[36] https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2012/03/15/zhuIndict.pdf

[37] https://www.justice.gov/nsd/files/export_case_list_june_2016_2.pdf/download

[38] https://www.justice.gov/sites/default/files/pages/attachments/2015/07/22/export-case-list-201505-final.pdf

[39] https://www.csmonitor.com/USA/2012/0914/Stealing-US-business-secrets-Experts-ID-two-huge-cyber-gangs-in-China

[40] https://www.armed-services.senate.gov/press-releases/sasc-investigation-finds-chinese-intrusions-into-key-defense-contractors

[41] https://www.justice.gov/opa/pr/michigan-man-sentenced-48-months-attempting-spy-people-s-republic-china

[42] https://www.wsj.com/articles/SB10001424052970204058404577110541568535300
[43] https://www.justice.gov/opa/pr/chinese-national-sentenced-87-months-prison-economic-espionage-and-theft-trade-secrets
[44] https://www.cio.com/article/2413391/man-charged-with-stealing-secrets-from-wireless-company-sirf.html
[45] https://www.justice.gov/usao-ndca/pr/four-chinese-state-owned-industrial-companies-arraigned-economic-espionage-conspiracy
[46] https://www.justice.gov/opa/pr/former-dow-research-scientist-sentenced-60-months-prison-stealing-trade-secrets-and-perjury
[47] https://www.justice.gov/opa/pr/chinese-company-sinovel-wind-group-convicted-theft-trade-secrets
[48] https://www.nytimes.com/2011/03/18/technology/18secure.html
[49] https://www.wired.com/2011/06/gmail-hack/; https://www.washingtonpost.com/blogs/post-tech/post/google-hundreds-of-gmail-accounts-hacked-including-some-senior-us-government-officials/2011/06/01/AGgASgGH_blog.html
[50] http://www.computerworld.com/article/2507715/cybercrime-hacking/oak-ridge-national-lab-shuts-down-internet--email-after-cyberattack.html
[51] https://www.justice.gov/nsd/files/export_case_list_june_2016_2.pdf/download
[52] https://www.reuters.com/article/us-cyberattacks/state-actor-behind-slew-of-cyber-attacks-idUSTRE7720HU20110803
[53] https://www.reuters.com/article/us-cyberattack-chemicals-idUSTRE79U4K920111031
[54]https://web.archive.org/web/20111124012100/http://www.uscc.gov/annual_report/2011/annual_report_full_11.pdf
[55] https://www.military.com/defensetech/2012/02/06/did-chinese-espionage-lead-to-f-35-delays; https://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html
[56] https://www.reuters.com/article/us-nasa-cyberattack/nasa-says-was-hacked-13-times-last-year-idUSTRE8211G320120303
[57] https://www.csmonitor.com/Environment/2013/0227/Exclusive-Cyberattack-leaves-natural-gas-pipelines-vulnerable-to-sabotage
[58] https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf
[59] https://www.justice.gov/usao-edva/pr/former-cia-officer-pleads-guilty-conspiracy-commit-espionage
[60] justice.gov/usao-ndca/pr/four-executives-bay-area-semiconductor-equipment-manufacturer-charged-alleged
[61] https://www.justice.gov/usao-nj/pr/former-employee-new-jersey-defense-contractor-sentenced-70-months-prison-exporting
[62] https://www.justice.gov/usao-wdmo/pr/chinese-business-owner-employee-plead-guilty-sentenced-stealing-trade-secrets-sedalia
[63] https://www.justice.gov/usao-cdca/pr/chinese-national-who-stole-trade-secrets-while-working-medical-device-companies
[64] https://www.sfchronicle.com/bayarea/matier-ross/article/Sen-Feinstein-had-a-Chinese-connection-she-13121441.php
[65] Ellen Nakashima, "Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies."; https://www.mic.com/articles/44897/defense-science-board-hacking-report-china-is-hacking-its-way-through-u-s-defenses
[66] https://www.nytimes.com/2013/02/02/technology/washington-posts-joins-list-of-media-hacked-by-the-chinese.html
[67] https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf
[68] https://www.crowdstrike.com/blog/whois-anchor-panda/
[69] https://www.pcworld.com/article/2037037/us-department-of-labor-website-infected-with-malware.html
[70] https://www.armed-services.senate.gov/press-releases/sasc-investigation-finds-chinese-intrusions-into-key-defense-contractors
[71] https://www.justice.gov/usao-edpa/pr/solar-technology-research-scientist-pleas-guilty-wire-fraud
[72] https://www.theregister.co.uk/2013/09/26/icefog_hit_and_run_apt_japan_south_korea/
[73] https://blog.trendmicro.com/trendlabs-security-intelligence/sykipot-now-targeting-us-civil-aviation-sector-information/
[74] https://www.fireeye.com/blog/threat-research/2013/10/know-your-enemy-tracking-a-rapidly-evolving-apt-actor.html

[75] https://www.justice.gov/usao-sdia/pr/six-chinese-nationals-indicted-conspiring-steal-trade-secrets-us-seed-companies
[76] https://www.justice.gov/opa/page/file/1122681/download
[77] https://www.justice.gov/nsd/page/file/1044446/download
[78] https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor
[79] https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf
[80] https://www.meddeviceonline.com/doc/ge-files-charges-against-chinese-engineer-for-stealing-trade-secrets-0001
[81] https://time.com/3148773/report-devastating-heartbleed-flaw-was-used-in-hospital-hack/
[82] https://www.justice.gov/usao-cdca/pr/los-angeles-grand-jury-indicts-chinese-national-computer-hacking-scheme-allegedly
[83] https://www.washingtonpost.com/world/national-security/dhs-contractor-suffers-major-computer-breach-officials-say/2014/08/06/8ed131b4-1d89-11e4-ae54-0cfe1f974f8a_story.html
[84] https://www.justice.gov/opa/press-release/file/1124996/download
[85] https://www.reuters.com/article/usa-china-espionage-idUSL1N0RJ02T20140918
[86] https://www.w ashingtonpost.com/news/federal-eye/wp/2014/11/10/china-suspected-of-breaching-u-s-postal-service-computer-networks/
[87] https://www.justice.gov/opa/pr/chinese-national-admits-stealing-sensitive-military-program-documents-united-technologies
[88] https://www.justice.gov/opa/pr/newly-unsealed-federal-indictment-charges-software-engineer-taking-stolen-trade-secrets-china
[89] https://www.justice.gov/opa/pr/member-sophisticated-china -hacking-group-indicted-series-computer-intrusions-including
[90] https://www.theguardian.com/technology/2015/mar/30/github-cleans-up-cyber-attack
[91] https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/
[92] https://www.justice.gov/usao-wdnc/pr/chinese-businessman-charged-theft-trade-secrets
[93] https://www.justice.gov/opa/page/file/1122681/download
[94] https://www.justice.gov/usao-wdpa/pr/former-ppg-employee-charged-theft-trade-secrets
[95] https://www.justice.gov/opa/pr/chinese-professors-among-six-defendants-charged-economic-espionage-and-theft-trade-secrets
[96] https://www.bloomberg.com/news/articles/2015-07-29/china-tied-hackers-that-hit-u-s-said-to-breach-united-airlines
[97] https://www.justice.gov/usao-ndil/pr/businessman-indicted-allegedly-stealing-employer-s-trade-secrets-while-planning-new-job
[98] https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-economic-espionage-charges-against-chinese-man-stealing
[99] https://www.justice.gov/usao-edpa/pr/second-former-glaxosmithkline-scientist-pleads-guilty-stealing-trade-secrets-benefit
[100] https://www.justice.gov/usao-sdny/pr/former-fbi-employee-sentenced-manhattan-federal-court-24-months-prison-acting-agent
[101] https://www.justice.gov/nsd/page/file/1044446/download
[102] https://www.apnews.com/957fced045b1624d5e3d46cba250125e
[103] https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-june-mustang-panda/
[104] https://www.justice.gov/opa/pr/former-state-department-employee-sentenced-conspiring-chinese-agents
[105] https://www.justice.gov/opa/page/file/1122681/download
[106] https://www.justice.gov/opa/page/file/1122681/download
[107] https://www.justice.gov/usao-ma/pr/dual-canadianchinese-citizen-arrested-attempting-steal-trade-secrets-and-computer
[108] https://blog.checkpoint.com/2017/06/01/fireball-chinese-malware-250-million-infection/
[109] https://www.wsj.com/articles/chinese-governments-battle-against-fugitive-guo-wengui-spills-into-washington-1507260255
[110] https://www.justice.gov/usao-de/pr/former-chemours-employee-charged-conspiracy-steal-trade-secrets-connection-plan-sell

[111] https://www.justice.gov/opa/pr/electrical-engineer-convicted-conspiring-illegally-export-china-semiconductor-chips-missile
[112] https://www.reuters.com/article/us-usa-china-cyber/china-hacked-sensitive-us-navy-undersea-warfare-plans-washington-post-idUSKCN1J42MM
[113] https://www.justice.gov/opa/page/file/1122681/download
[114] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets
[115] https://www.justice.gov/opa/pr/former-defense-intelligence-officer-pleads-guilty-attempted-espionage
[116] https://www.justice.gov/opa/pr/new-york-man-charged-theft-trade-secrets
[117] https://www.bizjournals.com/sanjose/news/2018/07/17/apple-employee-pleads-not-guilty-car-secrets-aapl.html
[118] https://www.politico.com/story/2018/12/12/pompeo-says-china-hacked-marriott-1059172
[119] https://www.justice.gov/opa/page/file/1122681/download
[120] https://www.justice.gov/opa/page/file/1122681/download
[121] https://www.justice.gov/opa/press-release/file/1132356/download
[122] https://www.scmp.com/news/world/united-states-canada/article/2179192/chinese-battery-expert-hongjin-tan-charged-stealing
[123] https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion
[124] https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion
[125] https://www.scmp.com/news/china/science/article/2184393/chinese-man-jizhong-chen-stole-apples-future-car-secrets-company
[126] https://www.wsj.com/articles/chinese-hackers-target-universities-in-pursuit-of-maritime-military-secrets-11551781800
[127] https://foreignpolicy.com/2019/03/24/china-and-russia-are-spying-on-israel-to-steal-u-s-secrets-putin-netanyahu-xi-haifa-ashdod-iai-elbit/
[128] https://www.justice.gov/opa/pr/former-ge-engineer-and-chinese-businessman-charged-economic-espionage-and-theft-ge-s-trade
[129] https://www.justice.gov/usao-ma/pr/lexington-man-and-semiconductor-company-indicted-theft-trade-secrets
[130] https://www.wsj.com/articles/global-telecom-carriers-attacked-by-suspected-chinese-hackers-11561428003

https://www.forbes.com/sites/zakdoffman/2019/08/03/chinese-state-hackers-suspected-of-malicious-cyber-attack-on-u-s-utilities/#7ff1e4f76758
[132] https://www.forbes.com/sites/zakdoffman/2019/08/03/chinese-state-hackers-suspected-of-malicious-cyber-attack-on-u-s-utilities/#56e5bc686758
[133] https://www.reuters.com/article/us-china-cyber-moonlighters/chinese-government-hackers-suspected-of-moonlighting-for-profit-idUSKCN1UX1JE; https://content.fireeye.com/apt-41/rpt-apt41/
[134] https://www.justice.gov/opa/pr/former-cia-officer-arrested-and-charged-espionage
[135] https://www.justice.gov/opa/pr/couple-who-worked-local-research-institute-10-years-charged-stealing-trade-secrets-wire-fraud
[136] https://www.justice.gov/opa/press-release/file/1202996/download
[137] https://www.justice.gov/opa/pr/chinese-government-employee-charged-manhattan-federal-court-participating-conspiracy
[138] https://www.justice.gov/opa/pr/former-intelligence-officer-convicted-attempted-espionage-sentenced-10-years-federal-prison
[139] https://www.justice.gov/opa/pr/former-intelligence-officer-convicted-attempted-espionage-sentenced-10-years-federal-prison
[140] https://www.justice.gov/opa/pr/former-cia-officer-sentenced-conspiracy-commit-espionage
[141] https://www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related
[142] https://www.justice.gov/opa/pr/chinese-citizen-convicted-economic-espionage-theft-trade-secrets-and-conspiracy
[143] https://www.justice.gov/opa/pr/researchers-charged-visa-fraud-after-lying-about-their-work-china-s-people-s-liberation-army

[144] https://www.justice.gov/opa/pr/singaporean-national-pleads-guilty-acting-united-states-illegal-agent-chinese-intelligence
[145] https://www.justice.gov/opa/pr/university-arkansas-professor-indicted-wire-fraud-and-passport-fraud
[146] https://www.justice.gov/opa/pr/nasa-researcher-arrested-false-statements-and-wire-fraud-relation-china-s-talents-program
[147] https://www.justice.gov/opa/pr/chinese-national-charged-destroying-hard-drive-during-fbi-investigation-possible-transfer
[148] https://www.justice.gov/opa/pr/new-york-city-police-department-officer-charged-acting-illegal-agent-people-s-republic-china
[149] https://www.axios.com/china-spy-california-politicians-9d2dfb99-f839-4e00-8bd8-59dec0daf589.html
[150] https://www.justice.gov/opa/pr/chinese-energy-company-us-oil-gas-affiliate-and-chinese-national-indicted-theft-trade-secrets
[151] https://www.justice.gov/opa/pr/university-researcher-pleads-guilty-lying-grant-applications-develop-scientific-expertise
[152] https://www.justice.gov/opa/pr/former-raytheon-engineer-sentenced-exporting-sensitive-military-related-technology-china