# Public Loss Collective

A growing library of known losses suffered by American entities at the hand of foreign nation-state adversaries.

Mechanism Key:

| Word/ phrase | Meaning |
|---|---|
| Insider Threat Actor | A person within an entity who is maliciously acting against company and USG interests (poses economic, technological, or IP risk). Includes:<br>• Covert theft of goods or IP<br>• Research exploitation<br>• Abuse of privilege<br>• Intentionally evading sanctions<br>• Intentionally hiding or concealing end-users of goods or IP |
| Threat Actor | A person NOT within an entity who is maliciously acting against company and USG interests (poses economic, technological, or IP risk). Includes:<br>• Covert theft of goods or IP<br>• Research exploitation<br>• Abuse of visiting/ information privilege |
| Human error/ negligence | A person within an entity who is acting against company and USG interests unintentionally (poses economic, technological, or IP risk). Includes:<br>• Ignoring warning signs to potential threats<br>• Lack of oversight/ due diligence for subsidiaries or foreign trading partners |
| Machine error | Automated processes that pose a threat to USG interests through inadequate/ faulty/ incomplete screenings |
| Venture Threat | A venture effort between two or more entities where one or more entities have malicious intent (poses economic, technological, or IP risk) toward another. Includes:<br>• Venture Capital<br>• Joint Venture<br>• Funding/ Deals |

| | |
|---|---|
| Cyber Attack | Malicious activity in an attempt to steal, take, or destroy information system resources or information itself. In some cases, the stolen information can be held for ransom. Includes:<br>• Malware<br>• Phishing<br>• Hacking<br>• Hijacking<br>• Formjacking<br>• Cryptojacking<br>• Zero-Day Exploit |

Library:

| Date | Status | Company/ Target | Target Country | Threat | Industry | Mechanism | Loss | Comments | Sources |
|---|---|---|---|---|---|---|---|---|---|
| 2018 | Convicted<br><br>(Violations 2011 - 2013) | AMSC (formerly American Superconductor Inc.) | USA | Sinovel Wind Group Co. Ltd. (dba Sinovel Wind Group (USA) Co. Ltd.); China | Power/ energy | Insider Threat Actors:<br>• Conspiracy<br>• Theft<br>• Cybertheft | Monetary loss: >$1B<br>• Shareholder Equity: >$1B<br>• Contract: >$800M in contracted products<br>• IP theft: Unknown<br><br>Job loss:<br>• Almost 700 people lost their job<br><br>IP theft:<br>• Wind turbine technology<br>• Company source code | Sinovel stole the IP and reproduced the product. | DOJ |
| 2018 | Sentenced | Phillips 66 | USA | Xiamen Tungsten; China | Oil and gas | Insider Threat Actor—Hongjin Tan:<br>• FTP TTP<br>• Economic Espionage | Monetary loss: >$1B<br><br>IP theft:<br>• >$1B in trade secrets | | FBI<br>FBI |
| 2022 | Accused | Ronin Network | USA | Lazarus Group; N. Korea | Cryptocurrency | Cyber Attack | Monetary loss: >$600M | | CNBC<br>Crypto<br>CNBC2 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 2021 | Charged<br><br>Violations (1999 - 2016) | Unnamed US companies<br><br>Unnamed US-based banks | USA | >70 Front Companies, often using the name “Persepolis” or “Rosco;” Iran<br><br>(These front companies were in the United States, Iran, Canada, the United Arab Emirates and Hong Kong); Hong Kong-based front company: Total Excellence Ltd. | Financial<br><br>Government<br><br>Defense<br><br>More | Inside threat actors + threat actors—Seyed Ziaeddin Taheri Zangakani; Saeed Torab Abtahi; Abbas Amin; Issa Shayegh; Mojtaba Deghani; Sara Sabri; Reza Karimi; Shantia Chupra; Salim Henareh; Khalil Henareh:<br>• Conspiracy<br>• Money Laundering<br>• Illegal exportation<br>• Wire fraud | Monetary loss: >$300M<br>• Two $25M oil tankers | They conspired with/ created more than 70 front companies<br><br>10 threat actors were charged | DOJ<br>DOJ |
| 2015 -16 | Confirmed | Uber | USA | Russia | Transportation Mobility | Venture Threat:<br>• $3.7B joint venture with internet company Yandex<br>• Deals w/ several allies: Gref’s Sberbank, LetterOne Holdings investment firm. | Monetary loss (for these efforts): >$250M<br><br>Reputation loss<br><br>Violate US anti-bribery laws? | Attempted to break into and operate in their market. | The Guardian<br>ICIJ<br>TWP |
| 2015 | Confirmed | Anthem | USA | Unnamed China-based hacking group; Fujie Wang | Insurance | Cyber Attack | Monetary loss: >$166M<br><br>IP theft:<br>• Personal data of 80M customers<br>• >$166M in | | FBI<br>threatpost |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | repayment for damages | | |
| 2021 | Sentenced | Coca-Cola<br><br>Eastman Chemical Co.<br><br>Dow Chemical Co.<br><br>PPG Industries Inc.<br><br>Shirwin-Williams Co. | USA | Weihai Jinhong Group; China | Beverage | Insider Threat Actor—Xiaorong (Shannon) You:<br>• Wire fraud<br>• Foreign talent program (FTP); Thousand Talents Program of China (TTP)<br>• Economic espionage | Monetary loss: >$120M<br><br>IP theft:<br>• Theft of trade secrets worth more than $120M | Also conspired with Liu Xiangchen to use stolen trade secrets to start a Chinese company.<br><br>Left to China. | DOJ<br>DOJ<br>WH<br>Bloomberg<br>CJ<br>CJ |
| 2018 | Convicted<br><br>Violations (2011-19) | Genetech | USA | JHL Biotech, Inc.; Taiwan / China | Biotech | Insider Threat Actor(s)—Xanthe Lam:<br>• Theft<br>• Conspiracy | Monetary loss: >$101M<br><br>IP Theft:<br>• Theft of trade secrets<br><br>Confidential/ Proprietary Information Theft | Racho Jordanov and Rose Lin are co founders of JHL and wittingly hired Lam at the same time they were employed at Genentech. All parties concealed Lam's employment by paying her husband, Allen. | DOJ |
| 2022 | Charged | ASML | USA<br><br>Netherlands | Dongfang Jingyuan Electron Ltd.; China<br><br>Xtal Inc.; Silicon Valley (front for Dongfang) | Semiconductor | Insider Threat Actor—Song Lan, Wanyu Li, and Zongchang Yu:<br>• Theft<br>• Conspiracy | Monetary loss: >$100M<br>• Took ASML >100M and 10 years to develop technology that (Xtal attained a $27M contract with Samsung from ASML's IP)<br><br>IP Theft:<br>• Software theft<br>• Trade secret theft<br>• Design theft | | Bloomberg<br><br>Charges |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 2022 | Alleged | Horizon | USA | Lazarus Group; N. Korea | Cryptocurrency | Cyber Attack | Monetary loss: $100M | | CNBC |
| 2021 | Charged<br><br>(Violations 2015-18) | General Electric (GE) | USA | Dongguan Tianyu Semiconductor Technology Co., Ltd.; China<br><br>Unnamed Chinese startup (didn't have a name; still forming) | Semiconductor | Insider Threat Actor—Yang Sui:<br>• Conspiracy<br>• Theft<br>• Espionage | Monetary loss: $100M<br>• Ng and Sui told potential investors for their startup that they had assets worth approx $100M<br><br>IP Theft:<br>• Trade secrets: research, development, design and manufacture of its silicon carbide metal-oxide semiconductor field-effect transistors (MOSFETs) | Chi Lung Winsman Ng lives in Hong Kong and was arrested for conspiring with someone inside GE to use stolen trade secrets to start their own company in China.<br><br>No evidence of a any technology transfer to Chinese companies<br><br>MOSFETs are used in aviation equipment and wind turbines for GE | DOJ<br>DOJ |
| 2006 | Sentenced | Ford Motor Company | USA | Beijing Automotive Company | Automotive | Insider Threat Actor—Xiang Dong Yu:<br>• Theft | Monetary Loss: $50-$100M<br>• Trade secret information worth $50-$100M<br><br>IP Theft:<br>• Trade secrets: system design specifications for Engine/ Transmission Mounting Subsystem, Electrical Distribution System, Electric Power Supply, Electrical Subsystem and Generic | | CSIS<br>FBI |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | • Body Module, etc.<br>• Yu copied some 4,000 Ford documents onto an external hard drive, including sensitive Ford design documents | | |
| 2013 | Confirmed | Las Vegas Sands Corporation | USA | Iran | Hospitality<br><br>Tourism | Cyber Attack | Monetary loss: >$40M<br>• Equipment costs and recovery: >$40M<br><br>Data theft:<br>• Stole customer data: credit card, Social Security, and drivers license numbers | The CEO, Sheldon Adelson, provoked attack when he advocated for stronger threats of nuclear attack against Iran | Axios<br>Verge<br>CNN<br>CFR |
| 2006 | Sentenced | General Motors | USA | Millennium Technology International Inc.<br><br>Chery Automobile; China | Automobile | Insider Threat Actor—Shanshan Du and Yu Qin:<br>• Conspiracy<br>• Theft<br>• Wire fraud | Monetary loss: >$40M<br>• Value of stolen documents estd. >$40M<br><br>IP theft:<br>• Trade secrets<br>• 16,000 GM files | They intended to use the technology they stole in a joint venture with Chery Automobile | CSIS<br>FBI |
| 2014 | Sentenced | DuPont | USA | USA Performance Technology Inc. (Chinese-owned front company)<br><br>Pangang; PRC | Paint Industry<br><br>Chemical | Insider Threat Actors—Walter Lian-Heen Liew, Robert Maegerl:<br>• Theft<br>• Economic espionage<br>• Bankruptcy fraud<br>• Tax evasion<br>• Conspiracy<br>• Tampering | Monetary loss: >$27.5M<br>• Profits to Liew: >$27.5 (stolen profits)<br><br>IP Theft:<br>• Chloride-route titanium dioxide production technology | | Bloomberg<br>FBI<br>DOJ |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 2022 | Confirmed<br><br>(Since 2020) | Over 1000 companies throughout the world | USA, Canada, Mexico, Argentina, Denmark, UK, Netherlands, Sweden, Germany, etc. | Conti; Russia | Healthcare<br><br>Engineering<br><br>Government<br><br>Law<br><br>Insurance<br><br>Telecommunic-ations<br><br>Oil and Gas<br><br>Manufacturing<br><br>etc. | Cyber Attack<br><br>Ransomware | Monetary loss: >$25M<br>• They have been known to ask for around $25M of companies, upwards of $40M; however, not all paid<br><br>IP theft:<br>• Leaked IP, trade secrets, data, etc. of all companies that did not pay ransom. | | Esentire<br>SecBLVD<br>BC<br>CS |
| 2021 | Charges Dropped | Massachusetts Institute of Technology (MIT) | USA | China | Semiconductor<br><br>Research<br><br>Education | Insider Threat Actor—Gang Chen:<br>• FTP<br>• Foreign funding (>$29M)<br>• Grant fraud | Monetary loss: >$19M<br>• Grant fraud: >$19M (DOE among others) | Chen provided technical and scientific expertise to China—sometimes directly to PRC government officials—and partook in at least 2 talent programs. Did not disclose any of this info when applying for federal grants.<br><br>Sent himself an email indicating his desire to promote PRC development.<br><br>Case dismissed because prosecutors received information that Chen was not obligated to disclose PRC affiliations.<br><br>Received approx $29M in foreign funding | DOJ<br>NYT |
| 2017 | Confirmed | UniEnergy | USA | Dalian | Technology | Human error/ | Monetary loss: >$15M | This tech that was | NPR |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| -21 | | | | Rongke Power Co. Ltd.; China | Batteries | negligence:<br>• US DoE gave the technology to China as part of a sublicense then a license transfer | • >$15M in taxpayer dollars<br><br>Technology/ Information loss:<br>• Vanadium redox flow battery | supposed to support the US economy now supports China.<br><br>US companies are attempting to get licenses to make the batteries but cannot. | |
| 2011 -19 | Charged | Harvard University | USA | Wuhan University of Technology; US professor recruited by China TTP | Nanoscience; research; education | Insider Threat Actor—Charles Lieber:<br>• FTP<br>• Foreign funding<br>• Grant fraud<br>• Tax fraud | Monetary loss: >$15M<br>• Grant fraud: >$15M (NIH) | “Obligated to work for WUT “not less than nine months a year” by “declaring international cooperation projects, cultivating young teachers and Ph.D. students, organizing international conference[s], applying for patents and publishing articles in the name of” WUT”<br><br>TTP paid over $150K and >$1.5M for research lab | CJ<br>FBI |
| 2020 | Confirmed | Smith’s Harlow | UK | Futures Aerospace; China | Aviation | Venture Threat:<br>• Deal between 2 companies | Monetary loss: >$8M<br>• Had to go into administration<br>• $8M for deal<br><br>IP theft<br>• Technology transfer<br>• Training | Struck a deal with Future Aerospace in 2017 but Futures has yet to pay and backed out of the deal (after acquiring what it wanted). | BBC<br>M15 Security Service<br>CNN<br>yourharlow |
| 2020 | Fined in 2020<br><br>(Violations 2012-16) | Berkshire Hathaway | USA | Iscar Kesici Takim Ticareti ve Imalati Limited Sirket (Turkish subsidiary)<br><br>Iranian | Manufacturing | Insider Threat Actor:<br>• Iscar Turkey knowingly engaged in transactions with | Monetary loss: >$4.3M<br>• OFAC violations: >$4M settlement for Hathaway<br>• >$380K value of | Self-disclosed by Berkshire after anonymous tip | UANR<br>USDT<br>USDT |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Government Entities | | people under the jurisdiction of Iranian governmen t.<br>• Purchased goods from Berkshire and other subsidiarie s of it to send to Iran | manufactured goods to Iran | | |
| 2020 | Sentenced | Ohio State University | USA | Thousand Talents; China | Medical research<br><br>Education | Insider Threat Actor—Song Guo Zheng:<br>• FTP TTP<br>• Grant fraud | Monetary loss: >$4.5M<br>• Grant fraud: $4.1M (NIH)<br>• Grant fraud: >$400K (Ohio State University)<br><br>IP Theft:<br>• Scientific trade secrets | Used approx. $4.1M in NIH grants to develop China's expertise under the guise of researching and teaching in the USA. Lied about China affiliation.<br><br>Caught while attempting to flee to China<br><br>"to develop China's expertise in the areas of rheumatology and immunology." | DOJ<br>DOJ |
| 2020 | (Violations 2012 - 2015) | Whitford Worldwide Company, LLC | USA | Whitford S.r.l. (subsidiary; Italy)<br><br>Whitford Yuzey Kaplamalari Sanayi ve Ticaret Limited Sirketi (subsidiary; Turkey)<br><br>Iran | Manufacturing<br><br>Cookware coating | Insider Threat Actor(s):<br>• Indirectly continue to supply goods to Iran by avoiding reference to the country and go through 3rd party distributors<br>• A US person had | Monetary losses: >$3.8M<br>• >$3M benefit to Iran<br>• OFAC violations; >$800K settlement for Whitford | | UANR<br>USDT |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | knowledge of actions | | | |
| 2020 | Charged (dismissed) | Cleveland Clinic | USA | Huazhong University of Science and Technology; China | Molecular medicine | Insider Threat Actor—Qing Wang:<br>• Grant fraud<br>• FTP | Monetary loss: $3.6M<br>• Grant fraud: $3.6M (NIH)<br><br>Potential IP theft | | FBI<br>DOJ |
| 2019 | Sentenced | Nationwide Children's Hospital Research Institute | USA | Beijing Genexosome; China | Exosome medical research<br><br>Education | Insider Threat Actors—Chen Li and Yu Zhou:<br>• Wire fraud<br>• Economic espionage<br>• FTP TTP<br>• Foreign funding | Monetary loss: >$2.6M<br>• >$2.6M in restitution; likely stole more than this<br><br>IP theft:<br>• 5 trade secrets (exosome research) | The couple received benefits from Chinese programs and participated in multiple talent programs.<br><br>They are said to have started their own unnamed Chinese company using this information, as well. | Rfa.org<br>DOJ<br>forbes |
| 2020 | Sentenced | Edsun Equipments | USA | Many Iranian companies, some specifically sanctioned their threat to US national security<br><br>Mahan Air Co., sanctioned for support of terrorist groups | Individuals | Insider Threat Actor—Joyce Eliabachus (Joyce Marie Gundran Manangan):<br>• Conspiracy<br>• Theft | Monetary loss: >$2M<br><br>Theft:<br>• At least 49 shipments with over 23.5K license-controlled aircraft parts from US - Iran<br>• Over $2M worth of aircraft components sent to Iran | | UANR<br>DOJ |
| 2008 | Sentenced | Apple | USA | Multiple suppliers in China, South Korea, and Taiwan | Technology | Insider Threat Actor—Paul Shin Devine:<br>• Theft<br>• Wire fraud | Monetary Loss: >$2M<br>• Suppliers paid >2.3M to Devine for his information<br><br>IP Theft:<br>• Information about Apple's upcoming products | Devine gave info to suppliers to give them an advantage in negotiations. | Businessinsider<br>bloomberg |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | • Provided pricing information<br>• Projected sales figures | | |
| 2003 | Sentenced | FBI | USA | China | Government | Insider Threat Actor—Katrina M. Leung:<br>• Theft<br>• Negligence<br>• Espionage | Monetary loss: >$1.8M<br>• Pay to Katrina M. Leung by FBI for Informant status: $1.8M<br><br>Threat to national security | An essential, top FBI informant also served the PRC. The informant had sexual relations with both of her FBI handlers; she would steal files from their briefcases, photocopy them, and pass them to PRC | Guardian<br>CSIS<br>DOJ |
| 2021 | Charged | University of Florida<br><br>National Institute of Health (NIH) | USA | Lin Yang; Deep Informatics; China | Biotechnology; education | Insider Threat Actor—Lin Yang:<br>• Wire fraud<br>• Grant fraud<br>• Economic espionage<br>• FTP TTP<br>• Foreign funding | Monetary loss: $1.75M<br>• Grant fraud: $1.75M (NIH)<br><br>IP theft | Lin Yang was an associate professor and researcher for UF who received grants from NIH for research. During grant period, he founded Deep Informatics in China and joined China's Thousand Talents Program (TTP); this remained undisclosed<br><br>Fled to China | DOJ |
| 2021 | Fined in 2021<br><br>(Violations 2013-18) | Alliance Steel, Inc. | USA | Unnamed Iranian engineering company | Manufacturing | Human error/ negligence:<br>• Alliance imported Iranian engineering services | Monetary loss: >$1.4M<br>• >$1M in benefits to Iran<br>• OFAC Sanction violation: >$400K settlement for Alliance | This is why people should conduct due diligence; negligence is another way you can be screwed—these foreign threats don't have to do anything if we have willing participants… If you need help with DD, that's what we are for.<br><br>Iran was the only | UANR<br>USDT |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | international country Alliance worked with | |
| 2018 | Confirmed | Ticketmaster | USA | Magecart; Unknown country of origin. Languages attributed to Magecart include (mostly) Russian, English, Arabic, Chinese, Portuguese, and Indonesian | Entertainment | Cyber Attack<br>• Formjack; Malicious JavaScript code to steal payment information | Monetary loss: >$1.25M<br>• Information Commissioner's Office (ICO) fine: £1.25M fine to Ticketmaster<br><br>Data theft:<br>• Credit card details of 9 million customers<br>○ Name, address, email, password, phone number, payment information | | ISTR Register Zdnet |
| 2021 | Charged<br><br>(Violations 2007 - 2009; 2012 - 2015) | Unnamed US manufacturer | USA | Avnet Asia Pte. Ltd.; Singapore | Power/ Energy | Insider Threat Actor (2007 - 2009):<br>• Conspiracy<br><br>Insider Threat Actor (2012 - 2015)—Cheng Bo:<br>• Conspiracy<br>• Illegal exporting | Monetary loss: >$1.15M<br>• Goods from USA → Hong Kong → China: >$800K<br>○ Power amplifiers<br>• Goods from USA → Hong Kong → China OR Iran: >$340K | Two different actors at two different times. | DOJ DOJ |
| 2019 | Convicted | Analog Devices, Inc. (ADI) | USA | Tricon MMIC LLC | Semiconductor | Insider Threat Actor(s)—Haoyang Yu and Yanzhi Chen:<br>• Wire fraud<br>• Theft | Monetary loss: "Millions of dollars"<br><br>IP theft:<br>• Hundreds of files<br>• Trade secret theft<br>• Schematic design and | The chip is used in aerospace and defense<br><br>Acquitted of "other counts of possessing stolen trade secrets, wire fraud, immigration fraud, and the illegal export | DOJ DOJ |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | • modeling files (worth millions)<br>• Prototype design of HMC1022A Microchip<br><br>Smuggling<br><br>Transporting stolen goods<br><br>Visa fraud | of controlled technology”<br><br>Yu previously worked at ADI before starting Tricon<br><br>Haoyang Yu aka: Jack Yu, Harry Yu, and Jack Tricon<br><br>Marketed and sold approx 20 ADI designs as his own<br><br>Smuggled export-controlled technology from the United States to Taiwan w/ o export licensing<br><br>Exported to Turkey and China | |
| 2020 | Indicted<br><br>(Violations 2009 - 2020) | DOE’s Hanford<br><br>Hundreds of companies, governments, non-governmental organizations, and individual dissidents, clergy, and democratic and human rights activists | USA<br><br>Additional affected countries: UK, Australia, Belgium, Germany, Japan, Lithuania, Netherland, Spain, Sweden, South Korea | Guangdong State Security Department of the Chinese Ministry of State Security and other Chinese agencies | High tech manufacturing<br><br>Medical device, civil, and industrial engineering<br><br>Business, educational, and gaming software<br><br>Solar energy<br><br>Pharmaceutical<br><br>Defense | Threat actors—Li Xiaoyu and Dong Jiazhi:<br>• Hacking<br>• Computer fraud<br>• Theft<br>• Conspiracy<br>• Identity theft<br>• Wire fraud | Monetary loss: “Millions of dollars” in IP<br><br>IP Theft:<br>• Terabytes of data<br>• Trade secrets from 8 victims:<br>○ Technology designs<br>○ Manufacturing processes<br>○ Test mechanisms and results<br>○ Source code<br>○ Pharm | Threat actors not only did this on behalf of PRC but also for personal financial benefit. | DOJ CJ |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | aceuti cal chemi cal structu res<br><br>National security threat | | |
| 2007 | Sentenced | Motorola Solutions Inc. | USA | Unnamed Chinese company that develops telecom tech for PLA | Telecommunic-ations | Insider Threat Actor—Hanjuan Jin:<br>• Theft | Monetary Loss: “Millions of dollars”<br>• “Millions of dollars” and years of research to develop their tech<br><br>IP Theft:<br>• Trade secrets relating to its proprietary iDEN technology<br>• More than 1,000 electronic and paper Motorola documents | Stopped in O’Hare International Airport with a 1-way ticket to China and Motorola IP documents. | Bloomberg FBI |
| 2009 | Sentenced | Ford Motor | USA | Beijing Automotive; China (China branch of a US company)—Direct competitor of Ford | Automotive | Insider Threat Actor—Xiang Dong “Mike” Yu:<br>• Theft | Monetary Loss: “Millions of Dollars”<br>• Ford spent millions of dollars and decades of research to develop what was stolen.<br><br>IP Theft:<br>• 4,000 documents on external drive<br>• Sensitive design documents | Stole Ford documents just before resigning to relocate to China for Beijing Automotive | Bloomberg DOJ |
| 2021 | Fined | JC Flowers & | USA | Sanctioned | Financial | Human error/ | Monetary loss: >$850K | “First Bank | UANR USDT |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Co. (Parent company) | | Iranian and Syrian programs<br><br>First Bank SA (Romania) | Services | negligence:<br>• First Bank SA indirectly exported financial services through US financial institution (JC Flowers & Co.) | • OFAC Violation of Iran and Syria sanctions: >$850K Settlement for JC flowers | processed 98 commercial transactions totaling $3,589,189 through U.S. banks on behalf of parties located in Iran and Syria. In 2018, after JC Flowers acquired a majority ownership interest in First Bank, First Bank processed Euro-denominated payments for persons located in Iran."<br><br>Indirect transfer of funds<br><br>Self-disclosed by bank.<br><br>Resulted from First Bank's lack of understanding of US sanctions | |
| 2020 | Confirmed<br><br>(Violations 2016) | Keysight Technologies, Inc. | USA | Anite Finland Oy (subsidiary)<br><br>Iran | Electronics | Insider Threat Actor(s):<br>• Finland subsidiary's VP and Regional Manager did not want to cease sales to Iran after the acquisition, so they continued to covertly sell to Iran using the UAE as a cover | Monetary loss: >$750K<br>• >$300K US goods sent to Iran<br>• OFAC violations: >$450K settlement for Keysight | | UANR<br>USDT |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 2020 | Case dismissed | Texas A&M University<br><br>NASA | USA | Guangdong University of Technology; PRC<br><br>Unnamed Chinese Company | Education<br><br>Research<br><br>Government | Insider Threat Actor—Zhengdong Cheng:<br>• Wire fraud<br>• FTP<br>• Hid affiliation with multiple Chinese Universities and the Chinese company he co-founded<br>• Grant fraud | Monetary loss: $750K<br>• Graft fraud: $750K (NASA)<br><br>(Assumed) IP theft | Would not have received any grant money if disclosed affiliation with a talent program. | DOJ<br>scmp |
| 2007 | Sentenced | Palo Verde Nuclear Generating Station | USA | Iran | Nuclear | Insider Threat Actor—Mohammad Reza Alavi:<br>• Theft<br>• Computer fraud<br>• Illegal export | Monetary loss: $400K<br>• Stolen software value: $400K<br><br>IP Theft:<br>• “3KeyMaster” software used for employee training | Shortly after Alavi gave notice of work termination, he downloaded the software to his personal laptop which he later accessed after he returned to Iran. | Fed Cases<br>DOJ |
| 2021 | Fined in 2021<br><br>(Violations 2013-17) | UniConrol, Inc. | USA | Two unnamed European companies<br><br>Unnamed Iranian company | Manufacturing | Human error/ negligence:<br>• Ignored/ failed to act on warning signs of European trading partners reexporting items to Iran | Monetary loss: >$200K<br>• OFAC Sanction Violation: >200K settlement | Iran was listed as a trading partner form the European companies | UANR<br>USDT |
| 2021 | Convicted<br><br>(Violations 2016 - 2020) | Southern Illinois University | USA | Shenzhen University; China<br><br>Natural Science Foundation of Guangdong | Education<br><br>Mathematics | Insider Threat Actor—Mingqing Xiao:<br>• Grant fraud<br>• Wire fraud | Monetary loss: >$150K<br>• Grant fraud: >$150K (National Science Foundation)<br><br>Potential IP theft | Hid the fact that he was already on payroll for a Chinese university from 2018 - 2023 and received Chinese state funding for his research. | DOJ<br>DOJ<br>DOJ |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Province; China | | | | | |
| 2022 | Sentenced<br><br>(Violations 2021) | Department of the Navy | USA | Diana and Jonathan Toebbe; USA<br><br>“Foreign government” | Government<br><br>Nuclear technology | Insider Threat Actor—Jonathan Toebbe:<br>• Theft of restricted data<br>• Conspiracy | Potential monetary loss: >$100K<br>• Buyer paid $100K for information<br><br>IP theft:<br>• Restricted data for design of nuclear powered warships<br>• US Navy documents | Mr. Toebbe worked for the Department of the Navy (Top secret security clearance) as a nuclear engineer and decided to sell a foreign government; however, that (unidentified) country alerted the USG. | DOJ<br>DOJ<br>CJ<br>CJ |
| 2021 | Sentenced<br><br>(Violations 2015 - 2019) | Unnamed manufacturing companies | USA | Northwestern Polytechnical University (NWPU); China | Technology<br><br>Underwater marine applications | Insider Threat Actor—Shuren Qin:<br>• Illegal exportation<br>• Visa fraud<br>• Money laundering<br>• Smuggling | Monetary loss: >$100K<br>• >$100K US goods to NWPU | Smuggled hydrophones to China via an illegitimate business he started in the USA, LinkOcean Technologies, LTD..<br><br>He exported more than hydrophones; remotely-operated side scan sonar systems, unmanned underwater vehicles, unmanned surface vehicles, robotic boats and hydrophones | DOJ |
| 2020 | (Violations 2011 - 2018) | Amazon.com | USA | No specific persons; however, countries include: Crimea, Iran, Syria, Cuba, North Korea, and Sudan | E-Commerce | Machine error:<br>• Automated sanctions screening processes didn't fully analyze transaction s or data;<br>○ Did not flag alternate spellings of names and | Monetary loss: >$100K<br>• OFAC Violations: >100K settlement for Amazon | Accepted and processed orders from people and places that are sanctioned<br><br>Most transactions were for low-value retail goods. The total transaction value was approx $269K and they still received a steep | UANR<br>USDT |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | places (ex. Crimea → Krimea)<br>○ Didn't flag orders to Embassies of sanctioned countries in 3rd countries | | settlement for something seemingly miniscule; DD is important | |
| 2020 | Sentenced | West Virginia University | USA | Chinese Academy of Sciences; US professor recruited by China TTP | Physics research<br><br>Education | Insider Threat Actor—James Patrick Lewis:<br>• Federal Program Fraud<br>• FTP TTP (recruited) | Monetary loss: >$20K<br>• >$20K WVU paid to Dr. Lewis<br><br>IP theft:<br>• Possible US trade secrets theft<br>• Possible proprietary information theft | Dr. Lewis studied molecular reactions in coal conversion. In 2017, he joined China's TTP w/o notifying the university. Because he was expected to teach abroad, he took paternity leave—didn't stay with the newborn baby; instead, went to China.<br><br>Dr. Lewis received benefits from program:<br>• ~ $143K living subsidy<br>• ~ $573K research subsidy<br>• ~ $86K salary | DOJ |
| 2021 | Confirmed | Colonial Pipeline | USA | DarkSide; Russian cybercriminal group | Fuel Pipeline | Ransomware attack | Monetary loss: 75 bitcoins<br>• 75 bitcoin paid to DarkSide in ransom<br>○ FBI recovered 63.7 of the bitcoin | | CJCJ |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | Affected 17 states with ground transportation of gas, diesel, jet fuel, etc. | | |
| 2021 | Fined in 2021<br><br>(Violations 2015-16) | Alfa Laval AB (ultimate parent company)<br><br>Alfa Laval Inc. (US subsidiary) | Sweden<br><br>USA | Alfa Laval Middle East Ltd.; UAE<br><br>Alborz Pakhsh Parnia Company; Iran (Alborz) | Energy | Insider Threat Actor:<br>• Conspiracy<br>• AL Middle East conspired with Dubai- and Iran-based companies to case US-base to indirectly export goods (Gamajet storage tank cleaner) from the US to Iran by listing a Dubai-based company as end-user | Monetary loss: >$16K<br>• OFAC Sanction Violations: >$16K settlement for Alfa Laval Inc. (USA)<br><br>US goods to Iran | Alfa Laval ME to pay >$400K settlement | Treasury.gov UANR USDT UANR |
| 2020 | Sentenced<br><br>(Violations 2012 - 18) | Emory University, GA | USA | Chinese Academy of Sciences; China<br><br>JInan University; China | Animal science | Insider Threat Actor: Li Xiao-Jiang:<br>• Tax fraud<br>• Grant fraud<br>• FTP; TTP | Monetary loss: unknown<br>• Grant fraud: unknown (NIH) | Jiang to repay >$35K to IRS and any additional penalties.<br><br>Earned >$500K income from China during years working for China; did not report. | DOJ Science dekalb |
| 2020 | Case dismissed | University of California, San Francisco (UCSF) | USA | PLA: China | Medical<br><br>Research | Insider Threat Actor—Xin Wang:<br>• Visa fraud<br>• PLA<br>• Conspiracy<br>• Grant fraud | Monetary loss: unknown<br>• Grant fraud: unknown (NIH)<br><br>IP theft:<br>• Admitting to | Falsely denied PLA affiliation (position rank similar to US Major)<br><br>Sent by Chinese military university to | DOJ Insiderhighered Latimes WP |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | duplicating UCSF supervising professor's work in China | observe layout of UCSF and bring back information on how to replicate | |
| 2021 | Confirmed<br><br>(Violations 2010 - 2014) | Unnamed financial institutions | USA | Huawei; China | Finance<br><br>Technology | Insider Threat Actor—CFO Wanzhou Meng:<br>• Financial fraud<br>• Wire fraud<br>• Conspiracy | Fraudulently transferred money to Iran through USA (approx. $100K). | | DOJ<br>DOJ |
| 2011 | Confirmed | RSA | USA | Comment Crew/ Shanghai Group; China | Computer security | Cyber Attack; malware infiltration | IP theft:<br>• Stole "seeds"—secret keys that are the foundational promise of security of the company. They were a core ingredient for SecurIDs<br><br>Reputation damage<br><br>National security threat | RSA is known for its SecurID token which is used by US intelligence agencies, military contractors, banks, etc. | Atlanticcouncil<br>Wired<br>NYT |
| 2006 | Confirmed | Department of Defense | USA | China | Government<br><br>Defense | Cyber Attack | IP Theft:<br>• Stole 10 to 20 terabytes of data<br>• Non-classified NIPRNet<br><br>Threat to national security | | CSIS<br>Govinfo brown.edu |
| 2007 | Confirmed (Denied by China) | Pentagon<br><br>US Air Force<br><br>Lockheed Martin | USA | PLA; PRC | Government<br><br>Defense | Cyber Attack | IP Theft:<br>• Many terabytes of data related to F-35 fighter jet<br>• Material related to US Air Force's F-22 Raptor, B-2 Stealth | | CSIS<br>EurAsian Times |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | Bomber, space-based lasers, missile guidance and tracking systems, and designs for nuclear submarines and anti-air missiles<br><br>National security threat | | |
| 2005 | Sentenced in 2020 | Northrop Grumman Corporation | USA | PRC<br><br>Individuals in Germany, Israel, and Switzerland | Aerospace<br><br>Defense | Insider Threat Actor—Noshir Sheriarji Gowadia:<br>• Espionage<br>• Theft<br>• Conspiracy | IP theft:<br>• When searching one of Gowadia's residences, authorities found 500 pounds of evidence<br>○ 40 boxes of US and foreign classified documents<br>○ 6 computers<br>○ Many thumb drives<br>○ Other electronic media with classified and restricted information<br>• B-2 Stealth bomber and other propulsion systems<br><br>Threat to national security and safety | Traveled to China six times to help government engineers to develop a Low Observable exhaust nozzle for their cruise missile. | OSI<br>OSI<br>CSIS<br>bloomberg |
| 2005 | Sentenced | Power Paragon<br><br>US Navy | USA | PRC | Government<br><br>Defense | Insider Threat Actor(s)—Chi Mak; Tai Wang Mak; | IP Theft:<br>• Current and future naval | He was a lead engineer on a defense project | DOJ<br>CSIS<br>CJ<br>bloomberg |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Rebecca Chiu; Yui Mak; Fuk Heung Li:<br>• Theft<br>• Illegal exportation<br>• Conspiracy<br>• Espionage | warship technology<br><br>Threat to national security | working on the propulsion of US Navy warships. He was also a defense contractor for the L-3 Power Paragon and helped develop Quiet Electric Drive Technology.<br><br>He is believed to have been dispatched to the US by Chinese intelligence | |
| 2005 | Arrested | Lockheed Martin | USA | PRC | Defense | Insider Threat Actor—Moo Ko-Suen:<br>• Illegal (attempted) exportation<br>• Money laundering<br>• Theft<br>• Conspiracy | IP theft:<br>• Attempt to smuggle sensitive technology grom the F-16 Falcon, an advanced fighter jet<br><br>Threat to national security | | CSIS<br>taipeitimes |
| 2006 | Confirmed | NASA<br><br>Lockheed Martin<br><br>Boeing | USA | PRC Hackers | Government<br><br>Aerospace<br><br>Defense | Cyber Attack | IP theft:<br>• Stole information about Space SHuttle Discovery program<br><br>Threat to national security | | CSIS |
| 2020 | Confirmed | SolarWinds | USA | Russia | Cybersecurity | Cyber Attack | IP theft<br><br>National security threat<br><br>Reputation damage | Affected 9 US federal agencies | Wired<br>NPR |
| 2006 | Confirmed | Department of Defense | USA | China | Government<br><br>Defense | Cyber Attack | IP Theft:<br>• Stole 10 to 20 terabytes of data | | CSIS<br>Govinfo<br>brown.edu |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | • Non-classified NIPRNet<br><br>Threat to national security | | |
| 2006 | Sentenced | Quantum3D<br><br>US Military | USA | Navy Research Center; PRC | Defense<br><br>Software<br><br>Government | Insider Threat Actor—Xiaodong Sheldon Meng:<br>• Theft<br>• Economic Espionage<br>• Export Violations | IP Theft:<br>• Military source code<br>• Military IP<br>• Trade secrets of Quantum3D | He was able to steal Military IP and trade secrets by the company he worked for, Quantum3D<br><br>viXsen is a Quantum3D visual simulation software program used for training military fighter pilots who use night visual sensor equipment, including thermal imaging.<br><br>Meng was assisting in developing two separate military proposals for two separate Air Forces in Southeast Asia involving visual simulation equipment and source code. | CSIS<br>DOJ |
| 2006 | Sentenced | Sun Microsystems, Inc.<br><br>Transmeta Corporation | USA | Supervision Inc.; China | Microchips | • Insider Threat Actors—Fei Ye and Ming Zhong: | IP Theft:<br>• Trade secrets for microprocessors | Stole trade secrets for the benefit of their own company, Supervision Inc.<br><br>Supervision was to provide a share of profits from the chips they made to the City of Hangzhou and the Province of Zhejiang which were funding Supervision<br><br>Supervision applied for funding from the National High Technology | CSIS<br>DOJ |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | Research and Development Program of China (AKA 863 Program.) | |
| 2018 | Charged<br><br>(Violations 2006 - 2018) | >45 Technology Companies | USA | APT 10; China<br><br>Huaying Haitai; China | Technology | Cyber Attack | IP theft:<br>• Trade secrets<br>• Confidential Business Information | | DOJ |
| 2021 | Convicted<br><br>(Violations 2013 - 2018) | A number of Aviation companies in the US and abroad<br><br>General Electric<br><br>Honeywell<br><br>Safran | <br><br>USA<br><br>USA<br><br>France | Chinese Ministry of State Security | Aerospace<br><br>Aviation | Threat actor Yanjun Xu:<br>• Recruited insider threat actors in companies to act as spies for China<br>• Economic Espionage<br>• Theft<br>• Conspiracy | IP Theft:<br>• Trade secrets | Insider Threat Actor with GE was caught early on and worked with the FBI to catch Xu.<br><br>This was the first Chinese intelligence agent to be arrested and extradited to the USA. | DOJ<br>DOJ<br>CJ<br>CJ<br>WCPO |
| 2020 | Charged | Boston University | USA | People's Liberation Army of China | Physics<br><br>Chemistry<br><br>Biomedical Engineering<br><br>Research<br><br>Dducation | Insider Threat Actor—Yanqing Ye:<br>• Agent of Chinese Military<br>• Visa fraud<br>• Conspiracy | IP theft:<br>• University research projects<br>• US documents<br>• US military projects | Ye is a Lieutenant of the People's Liberation Army of China who came to the USA as a student. Continues working for the PLA and a search of her devices says she accessed US military websites, researched their projects, and sent US documents to China. Also compiled information on 2 US scientists w/ expertise on robotics and CS. | Cbsnews<br>DOJ |
| 2017 | Confirmed | Equifax | USA | People's Liberation Army; China | Credit | Cyber Attack | IP theft<br>• User data; personal info on 150M | | FBI |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | Americans | | |
| 2014 | Confirmed | Office of Personnel Management (Gov't) | USA | Unknown Chinese state-sponsored group | Government | Cyber Attack | IP theft:<br>• User data: >21M Personal records | | FBI |
| 2021 | Confirmed | Microsoft | USA | HAFNIUM Group; Chinese state-backed hacking group<br><br>Various adversaries had access | Technology<br><br>Exchange servers | Cyber Attack | Affected >21K organizations<br>• User names, passwords<br>• IP theft<br>• Confidential information<br>• Blackmail material | | SecBLVD<br>Guardian<br>CJ<br>CNN |
| 2019 | Confirmed | T-Mobile | USA | Huawei; China | Telecommunic-ations | Insider Threat Actor:<br>• Recruiting competitor employees<br>• Professors at research institutions to obtain and provide technology<br>• Exploitation of Openness<br>• Conspiracy<br><br>Fraud<br><br>Breaking confidentiality agreements | IP theft:<br>• Source code<br>• User manuals<br>• Antenna technology<br>• Robot testing technology | Cut research costs for Huawei and gives competitive advantage | FBI<br>DOJ<br>Chicago Tribune |
| 2008 | Sentenced | Metaldyne | USA | Huafu; China | Manufacturing | Insider Threat Actor(s)—Anne Lockwood and Fuping Liu:<br>• Conspiracy<br>• Theft | IP Theft:<br>• Electronic and paper companies of information<br>• Production of powdered metal products | Provided info to Metaldyne's Chinese competitor, Huafu. | CSIS<br>DOJ |
| 2008 | Sentenced | Boeing | USA | PRC | Aerospace | Insider Threat | IP Theft: | First person in the | CSIS |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Rockwell Intl | | | | Actor—Dongfan Greg Chung:<br>• Theft<br>• Economic espionage | • 300,000 pages of sensitive papers in his home<br>○ US Space Shuttle<br>○ Delta IV Rocket<br>○ F-15 Fighter<br>○ B-52 Bomber<br>○ Chinook Helicopter | USA for economic espionage charges. | Bloomberg<br>Nbc news |
| 2011 | Sentenced | Chicago Mercantile Exchange (CME) Group | USA | Unnamed Business; China | Electronics | Insider Threat Actor—Chunlai Yang:<br>• Theft | IP Theft:<br>• Trade Secrets<br>• >10,000 files of computer source code and algorithms | | Bloomberg<br>reuters |
| 2010 | Sentenced | Dow AgroSciences<br><br>Cargill | USA | Universities in China | Biotechnology | Insider Threat Actor—Kexue Huang:<br>• Theft | IP Theft:<br>• Trade secrets about pesticides and components for new foods | | bloomberg |
| 2012 | Sentenced | Dow Chemical Company | USA | Numerous companies in China | Energy | Insider Threat Actor—Wen Chyu Liu:<br>• Theft<br>• Bribery | IP Theft:<br>• Dow's Tyrin CPE process and product technology<br>• Dow's process and product technology<br>• Secrets of making chlorinated polyethylene (CPE) used in vinyl siding, electrical cable jackets, and industrial hoses | Liu traveled through China to market the stolen information | Bloomberg<br>DOJ |
| 2010 | Sentenced | DuPont | USA | Peking University; China | Chemical | Insider Threat Actor—Hong Meng:<br>• Theft | IP Theft:<br>• Trade secrets;<br>○ Breakthrough chemical process about | Stole the chemical process knowing it would harm DuPont. Embedded it to a word file he put on a | Bloomberg<br>DOJ |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | ○ OLED displays<br>○ 109 Samples of trade secret chemical compounds | thumb drive, uploading it to his personal computer.<br><br>He sent the 109 samples to a friend at Northwestern University to send to China.<br><br>Meng secretly worked at Peking University while at DuPont. | |
| 2008 | Sentenced | EnfoTech | USA | Unnamed Chinese company | Software | Insider Threat Actor—Yan "Wesley" Zhu:<br>● Theft<br>● Wire fraud | IP Theft:<br>● Trade secrets<br>● Confidential and proprietary information<br>○ Computer systems and software with environmental applications | Zhu stole the IP to build their own software to sell in a couple provinces in China, including one where EnfoTech wanted to do business. | Bloomberg<br>DOJ |
| 2010 | Sentenced | Goodyear Tire & Rubber | USA | Wyko Tire Technology Incorporated; USA<br><br>Haohua South China Guilin Rubber Company Limited; China | Automotive | Venture Threat:<br>● Wyko had a $1.2M contract with Haohua<br><br>Theft—Clark Alan Roberts Sean Edward Howley:<br>● Got into Goodyear's facility and took pictures for their own gain to sell to Chinese company<br>● False pretenses<br>● Wire fraud<br>● Conspiracy | IP Theft:<br>● Images of Goodyear's tire-building equipment | Wyko agreed to sell a swab down device which they didn't have nor could they complete the design, so they schemed to steal the designs from Goodyear.<br><br>The two men went to Goodyear to service Wyko gear; instead, took photos of their swab down device, sending them to a subsidiary to create a similar piece of equipment. | Bloomberg<br>DOJ |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 2013 | Sentenced | L-3 Communications<br><br>DOD | USA | PRC | Government<br><br>Defense | Insider Threat Actor—Sixing Liu:<br>• Theft | IP Theft:<br>• Thousands of electronic files<br>○ Detailing performance and design of guidance systems for missiles, rockets, target locations, and UAVs | Stole the information and made it into a presentation at a tech conference sponsored in China (not authorized by L-3) | Bloomberg<br>DOJ |
| 2011 | Sentenced | Sanofi-Aventis | USA | Abby PharmaTech (US Subsidiary of a Chinese Chemical Company) | Healthcare | Insider Threat Actor—Yuan Li:<br>• Theft | IP Theft:<br>• Trade secrets related to the development of compounds that can potentially be used for future drugs | Li was a 50% partner at Abby. She stole the compounds and made them available for sale on the Abby website. | Bloomberg<br>DOJ |
| 2009 | Indicted | SiRF Technology | USA | Anywhere Logic, Inc.; China (locations: USA, Hong Kong, Beijing) | Software | Insider Threat Actor—Zhiqiang Zhang:<br>• Theft<br>• Foreign transportation (of stolen property)<br>• Recruit employees from victim company to competing one | IP theft:<br>• Software source code | After directing the software development of SiRF, he established a corporate entity, recruiting people who still worked at SiRF, for his own benefit. | Bloomberg<br>DOJ |
| 2019 | Indicted | GE Aviation (Subsidiary of General Electric) | USA | United Engine Corporation (UEC); Russia<br><br>Aviadvigatel (subsidiary of UEC); Russia | Aviation | Insider Threat Actor(s)—Maurizio Paolo Bianchi:<br>• Conspiracy<br>• Theft<br><br>Threat actor—Alexander Yuryevich Korshunov: | IP Theft:<br>• Trade secrets<br>• Jet engine accessory gearboxes | Bianchi worked at an Italian branch of GE Aviation. After he left, he went to a new company called Aernova where they had a contract with a US entity listed Aviadvigatel. At this time, Bianchi began | Fed Cases<br>DOJ<br>FBI |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | • Conspiracy<br>• Theft | | to hire current and former GE employees for consulting on a jet engine gearbox for them. Employees used GE trade secrets to create technical reports. | |
| 2016 | Sentenced | Boeing | USA | N/A<br><br>(Supposed to be Russia) | Aerospace | Insider Threat Actor—Gregory Allen Justice:<br>• Theft<br>• Economic espionage | IP Theft:<br>• Trade secrets<br>• Sensitive satellite information | Justice sold Boeing secrets to what he believed to be a Russian spy; however, was instead an undercover FBI agent. | Fed Cases<br>LATimes<br>DOJ |
| 2014 | Sentenced | Microsoft | USA | N/A<br><br>(Leaked by Russian national to a French blogger) | Software | Insider Threat Actor—Alex Kibkalo:<br>• Theft | IP Theft:<br>• Trade secrets<br>• Windows 8 proprietary software | People joke because Windows 8 was a flop anyways… | Fed Cases<br>Atlantic<br>NYT<br>DOJ |
| 2019 | Indicted | Ypsilanti<br><br>University of Michigan Energy Institute (assumed) | USA | Iran | Automotive<br><br>Aerospace | Insider Threat Actor—Amin Hasanzadeh:<br>• Theft<br>• Fraud<br>• Visa fraud | IP Theft:<br>• Trade secrets<br>• Hundreds of products | Transferred confidential data and products to his brother in Iran. His brother worked for a host of concerning Iranian companies, some overseen by the Ministry of Defense and Armed Forces Logistics | Fed Cases<br>LinkedIN<br>Iranwatch<br>NPR |
| 2019 | Indicted | Electro-Motive Diesel | USA | Tongmei (Gateway to America) Futures Exchange Software Technology; China | Locomotive manufacturing | Insider thrift actor—Xudong Yao:<br>• Theft | IP Theft:<br>• Over 3000 unique electric files with trade secrets and proprietary information<br>• Technical documents | Downloaded most trade secrets within the first two weeks of employment, then more as time went on.<br><br>He intended to start his own company, | Fed Cases<br>DOJ<br>Chicago Tribune |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | • Source code | Tongmei<br><br>In China | |
| 2018 | Guilty Plea | Apple, Inc. | USA | X-MOTORS; China | Consumer electronics<br><br>(Automobile) | Insider Threat Actor—Xiaolang Zhang:<br>• Theft | IP Theft:<br>• 25-page document with schematic drawings of critical infrastructure for apple car. | Investigations into Zhang began when he reported that he would travel to China to visit and take care of his ill mom. Apple launched an immediate forensic analysis. They discovered he would work at a China-based competitor's company and he downloaded information from project databases | Fed Cases<br>DOJ<br>Aljazeera<br>Chicago Tribune |
| 2001 | Sentenced | Lucent | USA | Datang Telecom Technology Company; China | Telecommunic-ations | Venture threat & Insider Threat Actors—Hai Lin, Kai Xu, and Yong-Qing Cheng:<br>• Theft<br>• Wire fraud<br>• Conspiracy | IP theft:<br>• Trade secret theft | Threat actors used stolen material to create their own Chinese company | CSIS.org<br>DOJ |
| 2004 | Sentenced | 3DGeo Development, Inc. | USA | PetroChina/ DaQing Oil; China | Software<br><br>Oil and gas | Insider Threat Actor—Yan Ming Shan:<br>• Theft<br>• Fraud<br>• Conspiracy | IP Theft:<br>• Software programs<br>• Source code<br>• Attempted to bring tech back to China | Yan Ming Shan was sent by one of 3DGeo's customers, PetroChina, for training where he gained unauthorized access to their computer system with an intent to defraud the company. | DOJ<br>CSIS |
| 2006 | Sentenced | NetLogic Microsystems<br><br>Taiwan Semiconductor | USA<br><br>Taiwan | SICO Microsystems Inc. | Microchips | Insider Threat Actors—Lan Lee and Yuefei Ge:<br>• Economic espionage | IP theft:<br>• Trade secrets | Threat actors intended to create their own company (SICO), using the | CSIS<br>DOJ |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Manufacturing Corporation | | | | • Theft<br>• FTP | | stolen trade secrets.<br><br>They would obtain venture capital funding from PRC by the 863 Program—a funding plan encouraging PRC scientists to develop advanced technologies—and the General Armaments Department—responsible for developing weaponry for the military. | |
| 2006 | Sentenced | Quantum3D<br><br>US Military | USA | Navy Research Center; PRC | Defense<br><br>Software<br><br>Government | Insider Threat Actor—Xiaodong Sheldon Meng:<br>• Theft<br>• Economic Espionage<br>• Export Violations | IP Theft:<br>• Military source code<br>• Military IP<br>• Trade secrets of Quantum3D | He was able to steal Military IP and trade secrets by the company he worked for, Quantum3D<br><br>viXsen is a Quantum3D visual simulation software program used for training military fighter pilots who use night visual sensor equipment, including thermal imaging.<br><br>Meng was assisting in developing two separate military proposals for two separate Air Forces in Southeast Asia involving visual simulation equipment and source code. | CSIS<br>DOJ |
| 2006 | Sentenced | Sun Microsystems, Inc.<br><br>Transmeta | USA | Supervision Inc.; China | Microchips | Insider Threat Actors—Fei Ye and Ming Zhong: | IP Theft:<br>• Trade secrets for microprocessors | Stole trade secrets for the benefit of their own company, Supervision Inc. | CSIS<br>DOJ |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Corporation | | | | | | Supervision was to provide a share of profits from the chips they made to the City of Hangzhou and the Province of Zhejiang which were funding Supervision<br><br>Supervision applied for funding from the National High Technology Research and Development Program of China (AKA 863 Program.) | |
| 2007 | Sentenced | Oak Ridge National Laboratory<br><br>Los Alamos National Laboratory<br><br>National Nuclear Security Administration | USA | PRC | Government<br><br>Defense; Atomic Weapons | Cyber Attack | IP Theft | | CSIS |
| 2008 | Sentenced | AkzoNobel | USA<br><br>Netherlands | Unnamed company in China | Paint Industry | Insider Threat Actor—Qinggui Zang:<br>• Theft | IP Theft:<br>• Formula for an industrial epoxy-based, fireproof coating | Papers found under insulation in attic space. | CSIS bloomberg |
| 2007 | Confirmed (Denied by China) | Pentagon<br><br>Secretary of Defense | USA | PLA; PRC | Government<br><br>Defense | Cyber Attack | Theft of confidential and private information:<br>• Computer system serving US Defense Secretary Robert Gates<br><br>National Security Threat | | CSIS csmonitor |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 2008 | Partially confirmed | US Secretary of Commerce | USA | PRC | Government | Threat Actor & Cyber Attack:<br>• Spyware installment | Threat to national security<br><br>Theft of personal data | PRC said to have installed spyware into then-U.S. Secretary of Commerce, Carlos Gutierrez while traveling on business. | CSIS<br>FP |
| 2007 | Confirmed | Department of Homeland Security | USA | PRC | Government<br><br>Defense | Cyber Attack | Theft of confidential and private information<br><br>National Security Threat | | CSIS |
| 2006 | Confirmed | US State Department | USA | China | Government | Cyber Attack | Threat to national security:<br>• Stole sensitive information and passwords from unclassified networks (mostly stole from offices of East Asia Affairs) | | CSIS<br>CNN |
| 2008 | Sentenced | Pentagon | USA | Ministry of State Security; PRC | Government<br><br>Defense | Human Error/ Negligence—Gregg W. Bergersen:<br>• Provided sensitive information to Mr. Kuo, believing he was a Taiwanese native, a US ally<br><br>Threat Actor—Tai Shen Kuo:<br>• Theft<br>• Conspiracy<br>• False identity | Threat to national security:<br>• Theft of confidential and private information related to US military sales to Taiwan and US military communication s security | Mr. Bergersen expressed embarrassment for his failed efforts to ensure continuation of a military relationship with Taiwan.<br><br>Kuo wined and dined Bergersen. Also led Bergersen to believe that he would make Bergersen a part owner or an employee of a company selling U.S. defense technology to Taiwan after Bergersen's retirement from | CSIS<br>DOJ<br>NYT |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | government service. | |
| 2006 | Confirmed | US Naval War College | USA | PLA; PRC | Government<br><br>Defense | Cyber Attack | National Security Threat | The college had to go offline for some time.<br><br>They attacked one of the website's colleges dedicated to training senior officers and developing cyberspace strategies. | CSIS<br>fcw.com |
| 2021 | Confirmed | Pulse Connect Secure (Parent company: Ivanti) | USA | APT5; Chinese state-backed hacking group | Cybersecurity | Cyber Attack | National security threat<br>• At least 5 government agencies breached; US Industrial Base vulnerable<br>○ Potential for more: 24 federal civilian agencies used | | CNN<br>CJ<br>CJ |
| 2004 | Sentenced | DIA | USA | People's Liberation Army of China | Government | Insider Threat Actor—Ronald N. Montaperto:<br>• Espionage<br>• Mishandling classified documents<br>• Conspiracy | Threat to national security:<br>• Passed classified documents to China's PLA | | CSIS<br>dhra.mil |
| 2005 | Confirmed | Numerous US Government Agencies | USA<br><br>UK | Titan Rain; Chinese hacking group | Government<br><br>Defense | Cyber Attack | Threat to national security<br>• Breached unclassified networks of US and UK Government departments | | CSIS<br>cfr.org |
| 2021 | Indicted | Dozens of unnamed | USA | Hainan Xiandun | Aviation | Cyberattack by threat actors Zhu | IP theft (including trade secrets, | These efforts would yield a | Justice.gov |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | (Violations 2011 - 2018) | companies, universities, and Government entities in USA<br><br>National Institutes of Health | (Additional targeted countries): Austria, Cambodia, Canada, Germany, Indonesia, Malaysia, Norway, Saudi Arabia, South Africa, United Kingdom, Switzerland | Technology Development Co., Ltd. (海南仙盾); China<br><br>Front company for hacking group with the following names: Advanced Persistent Threat (APT) 40, BRONZE, MOHAWK, FEVERDR-EAM, G0065, Gadolinium, Green Crash, Hellsing, Kryptonite Panda, Leviathan, Mudcarp, Periscope, Temp. Periscope, Temp. Jumper. | Government<br><br>Education<br><br>Defense<br><br>Healthcare<br><br>Biopharmaceutical<br><br>Maritime | Yumin, Wu Shurong, Ding Xiaoyang and Cheng Qingman:<br>• Malware<br>• Cyber espionage<br>• Spearphishing emails (with link to doppelgangers of legitimate companie-s) | confidential business information, and sensitive technologies):<br>• Infectious disease research:<br>○ Ebola<br>○ MERS<br>○ HIV/AIDS<br>○ Marburg<br>○ Tularemia<br>• Sensitive technologies<br>○ Submersibles<br>○ Autonomous vehicles<br>○ Specialty chemical formulas<br>○ Commercial aircraft servicing<br>○ Proprietary genetic-sequencing technology and date<br>• Froreign information to support Chinese contracts with the targeted country (e.g., railway development projects)<br>• Government knowledge/ information | significant economic benefit to China<br><br>Threat actors were part of Chinese Ministry of State Security (MSS)<br><br>Similar front companies affiliated with APT40: Hainan Yili, Hainan Tengyuan, Hainan Kehua, Hainan Yanwu, Hainan Dingwei, Haikou Fengshang, Hainan Hualian Anshi, Hainan Jiaxi, Hainan Xinhuaheng, Haikou Jianhui Li, Hainan Xin Yousheng and Haikou Xindahai | Justice.gov Justice.gov Clearancejobs Clearancejobs Wcpo Financialtimes scmagazine |
| 2021 | Sentenced<br><br>(Violations | US Military<br><br>NSA | USA | Main Directorate of the | Government | Insider threat actor—Peter Debbins: | Threat to national security/US intelligence: | | Justice.gov clearan |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | 1996 - 2019) | DIA<br><br>NATO | | General Staff of the Armed Forces of the Russian Federation/ GRU; Russia | | • Espionage<br>• Conspiracy | • Provided info about dis deployments and personnel from Military<br>• Information stolen from NSA, DIA, and NATO has not been disclosed | | cejobs |
| 2020 | Charged<br><br>(Violations 2004 - 2010) | FBI<br><br>CIA | USA | China's Ministry of State Security | Government | Insider Threat Actors—Alexander Yuk Ching Ma and an unnamed relative:<br>• Theft<br>• Insider information sharing<br>• Conspiracy<br>• Espionage | Threat to national security/ US intelligence:<br>• Provided info about the CIA and its activities related to China from when he worked there 12 years prior:<br>○ International operations<br>○ Cryptographic info used in classified and sensitive communications/ reports<br>○ Internal structure and organization of CIA<br>○ Officer identities<br>○ Human assets<br>○ Operational tradecraft<br>○ Technical departments<br>○ Communication practices<br>○ Staffing practices | The FBI sent an undercover agent to pose as a MSS and Ma said, "he wanted to see the motherland succeed." | DOJ<br>CJ |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | • Became a contract FBI linguist for Honolulu Dept to provide more info:<br>○ Discs of photos of documents<br>○ Photos of translated documents<br>○ Photocopies of translated documents<br>○ Digital storage device into his FBI computer | | |
| 2021 | Sentenced<br><br>(Violations 2019 - 2020) | USG<br><br>US Army; International task force | USA | Hezbollah; Lebanon | Government | Insider Threat Actor—Mariam Taha Thompson:<br>• Conspiracy<br>• Terrorism espionage<br>• Theft | National security threat:<br>• Accessed top secret/ confidential files that contained human intelligence sources:<br>○ True names<br>○ Personal identification data<br>○ Background information and photographs<br>○ Operational cables the assets provided to USG<br>○ Tactics, techniques, and procedures (TTPs) | Mariam was a contract linguist for USG in Iraq. | DOJ<br>TWP |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 2020 | Case dismissed | University of California, Los Angeles (UCLA) | USA | People's Liberation Army (PLA); China | Research<br><br>Education<br><br>Mathematics | Insider Threat Actor—Guan Lei:<br>• Technology / software transfer<br>• Visa fraud<br>• PLA | Potential IP theft | Lei was in the USA with a J-1 visa.<br><br>He threw the damaged hard drive into a dumpster after not being allowed to board a flight to China after refusing an examination of his computer.<br><br>Falsely denied association with Chinese military and potentially transferred data to China's National University of Defense Technology | DOJ |
| 2020 | Case dismissed | University of California at Davis | USA | PLA; China | Medical<br><br>Research | Insider Threat Actor—Juan Tang:<br>• Visa fraud<br>• PLA | (Assumed) IP theft | Dismissed because FBI agents had not informed Tang of her right against self-incrimination<br><br>Made false statements about affiliation with PLA | DOJ Insiderhighered Latimes TWP |
| 2020 | Case dismissed | Indiana University Bloomington | USA | PLA; China | Technology<br><br>Research | Insider Threat Actor—Zhao Kaikai:<br>• Visa fraud<br>• PLA | (Assumed) IP theft | Falsely denied PLA affiliation | DOJ Insiderhighered Latimes TWP |
| 2020 | Case dismissed | Stanford University | USA | PLA; China | Medicine<br><br>Research<br><br>Education | Insider Threat Actor—Song Chen:<br>• PLA<br>• Visa fraud | (Assumed) IP theft | Falsely denied PLA affiliation | DOJ DOJ Insiderhighered Latimes TWP |
| 2020 | Case dismissed | University of Tennessee<br><br>NASA | USA | Beijing University of Technology; China | Education<br><br>Research<br><br>Aerospace | Insider Threat Actor—Anming Hu:<br>• Wire fraud<br>• Grant fraud<br>• Collaborated with | Unknown monetary loss<br>• Grant NASA | | DOJ |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Chinese Universities | | | |
| 2020 | Charged | Unnamed US telecom company | USA | PRC | Telecommunic-ations | Insider Threat Actor—Xinjiang Jin:<br>• Conspiracy<br>• Theft<br>• Evidence fabrication | Theft of personal information<br><br>Defamation of employees of unnamed US telecom company<br><br>Free speech | | DOJ<br>DOJ |
| 2017 | Charged<br><br>Some sentencing | Yahoo | USA | Russian Federal Security Service | eMail | Cyber Attack | Data theft:<br>• Information from at least 500 million Yahoo users | Hackers used information from the Yahoo hack to access accounts at Yahoo, Google, and other email providers (focused on accounts of Russian journalists, US and Russian government officials, and private sector employees in finance, transportation, etc.) | Fed Cases<br>DOJ<br>DOJ |
| 2020 | Sentenced | West Virginia University<br><br>Synfuels Americas Corporation | USA | Energy Unitedy; (front company) PRC | Education<br><br>Research | Insider Threat Actor—Qingyun Sun:<br>• Tax fraud<br>• Wire fraud | (Potential) IP theft<br><br>Unknown monetary loss | | DOJ |
| 2020 | Sentenced | Los Alamos National Laboratory; DOE | USA | PRC | Nuclear Technology | Insider Threat Actor—Turab Lookman:<br>• FTP; TTP | (Potential) IP theft | | DOJ |
| 2018 | Dismissed (for prejudice) | Michigan State University | USA | City University of Hong Kong (CUHK); China | Education<br><br>Research | Insider Threat Actor—Ning Xi | Potential threat to IP | Xi violated MSU policy when he accepted a tenured pOSItion at CHUK. Alleged fabricated travel reimbursements as well | Fed Cases<br>apajustice |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 2019 | Confirmed | Moffitt Cancer Center<br><br>University of South Florida | USA | PRC | Medical Research | Insider Threat Actor(s)—Thomas Sellers (director); Alan List (CEO); Howard McLeod (researcher); Pearlie Epling-Burnette (researcher); Daniel Sullivan (head of clinical science program; and Sheng Wei (researcher)<br>• FTP; TTP<br>• Grant fraud | Unknown monetary loss:<br>• NIH Grant<br><br>(Potential) IP theft | Moffitt discovered at least six people (researchers and C-suite) with undisclosed Chinese affiliation and fired them all (or forced resignation). Involvement includes Thousand Talents Program (for all), working commercially and academically (outside of Moffitt) with Chinese nationals, recruited for TTP (both in and out of Moffitt), received foreign payment with foreign personal bank accounts, and supplied information from w/ in the institution. | Moffitt science org |
| 2020 | Sentenced | UE Canada Inc. (freight company)<br><br>Unnamed US companies | Canada<br><br>USA | Unnamed Iranian company (-ies) | Energy<br><br>Oil and gas | Insider Threat Actor—Angelica O. Preti:<br>• Illegally exported gas turbine engine parts | US goods to Iran | Behrooz Behroozian for similar charges | UANR<br>DOJ<br>NP<br>TWP |
| 2017 | Sentenced; potential harm | USG; NSA | USA | Reality Winner; Contractor for NSA<br><br>(Information valuable to foreign adversaries, especially Russia) | Government | Insider Threat Actor—Reality Winner:<br>• Illegally shared a classified/ top secret document with a news outlet | Classified documents/ information turn public:<br>• Exposed sources and methods used to gather intelligence on Russia's election interference<br>• Could have put intelligence officer lives at | | CJ<br>DOJ |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | stake | | |
| 2020 | Sentenced<br><br>(Violations 2018 - 2020) | Government agencies, non-government organizations, companies | USA | China's Ministry of State Security and the People's Liberation Army | Government | Threat actor—Jun Wei Yeo:<br>• Used social media, specifically LinkedIn to build contacts for China | Potential consequence to US intelligence | He created a fake company that was looking for consulting candidates. He received over 400 resumes and 90% of them were government employees with security clearances. | CJ<br>CJ<br>DOJ |
| 2022 | Charged | Chen Weiming (PRC national residing in Los Angeles) | USA | PRC | Art | Threat actors—Fan Liu, Matthew Ziburis, Qiang Sun, Craig Miller, and Derrick Taylor:<br>• Conspiracy<br>• Espionage<br>• Theft<br>• Stalking<br>• Harassing | Destruction of one's art (first sculpture was burned down)<br><br>Invasion of privacy. | | DOJ<br>DOJ<br>NPR |
| 2022 | Charged | Twitter | USA | Kingdom of Saudi Arabia | Social media | Insider Threat Actor—Ahmad Abouammo:<br>• Falsifying records<br>• Money laundering<br>• Wire fraud<br>• conspiracy | Invasion of Privacy:<br>• Accessed private information of Twitter users who were critical of Saudi Arabian regime, including:<br>○ IP addresses<br>○ Emails<br>○ Phone numbers<br>○ Birth dates | | DOJ<br>DOJ |
| 2022 | Potential | Hadean<br><br>In-Q-Tel | UK<br><br>USA | Tencent; China | Technology<br><br>Software | Venture threat<br>• Tencent, a Chinese company, is partially funding the developme-nt of this software. | Potential consequence of software theft/ loss | Per 2017 Chinese intelligence law, that company must share that information with the government | Telegraph<br>techforyou |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 2022 | Potential | Vehicle drivers | USA | MiCODUS; China | Transportation Systems | Cyber Attack | Potential consequence to US Cyber and National Security<br>• Supply routes<br>• Troop movement<br>• Recurring patrols<br>• Enable or disable a vehicle, monitor speed, routes, and other features | Cyber Hijacking via GPS Device:<br><br>MV720 GPS, created by MiCODUS allows access to vehicles | SecAffairs<br>CISA |
| 2022 | Potential | Apple | USA | Potential: NSO Group; Israel<br><br>Any hacker | Technology | Cyber Attack | Potential for hacker to get “full admin access” to a device | | NPR |
| 2022 | Potential | Grand Forks Air Force Base | USA | Fufeng Group; China | Military<br><br>UAV | Threat Actor:<br>• Electronic surveillanc-e | Potential consequence to intelligence. | “Could offer Chinese intelligence uNPRecedented access to the facility.”<br><br>Chinese graduates are asked to research the institution, research contracts, and individuals. | CNBC<br>American militaryne ws |
| 2020 | Sentenced; unconfirmed / potential harm<br><br>(Committed 2011 - 2018) | USG; DOD | USA | Asia Janay Lazarello; Citizen employee of DOD<br><br>(Potential for two Filipino nationals to have access to the documents) | Government | Insider Threat Actor—Asia Janay Lazarello:<br>• Stole/ took home piles of classified/ top secret paperwork that she printed | Potential consequence to intelligence/ stolen classified materials | She was hosting a dinner party with 5 people, including the two Filipino people. She was caught out of sheer luck. | CJ<br>CJ |
| 2019 | Sentenced | General Electric Power & Water | USA | Liaoning Tianyi Aviation | Power, Water, and Energy | Insider threat actor—Xiaoqing Zheng: | IP Theft:<br>• Trade secrets<br>• Electronic | | Fed cases<br>DOJ<br>DOJ |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Technology Co., Ltd. (LTAT); China<br><br>Nanjing Tianyi Avi Tech Co. Ltd. (NTAT); China | | • Theft<br>• Conspiracy<br>• Wire transfer<br><br>Threat actor—Zhaoxi Zhang:<br>• Advanced owned companies in China w/stolen secrets | Files<br>○ Design Models<br>○ Engineering Drawings<br>○ Configuration Files<br>○ Material Specifications | | |
| 2019 | Not Guilty Plea (Aug 2022) | Apple, Inc. | USA | China-based autonomous vehicle company; direct Apple competitor (Potentially: X-MOTORS; China) | Consumer Electronics<br><br>(Automobile) | Insider threat actor—Jizhong Chen:<br>• Conspiracy<br>• Theft | IP Theft:<br>• Trade Secrets<br>• ~100 photographs in sensitive work space<br>• Thousands of files with Apple IP: manuals, schematics, and diagrams | | Fed cases<br>AJ<br>NBCBA |
| 2018 | Confirmed | Micron Technology | USA | Jiangsu Province Ministry of State Security ("JSSD") and People's Republic of China's Ministry of State Security ("MSS")<br><br>Fujian Jinhua Integrated Circuit Co.<br><br>United Microelectro-nics Corp<br><br>Taiwan | Semiconductor Manufacturing | Cyber Attack<br>• Hacking<br><br>Threat actors—Zhang Zhang-Gui, Liu Chunliang, Gao Hong Kun, Zhuang Xiaowei, Zha Rong, Chai Meng, and Ma Zhiqi:<br>• Theft<br>• Conspiracy | IP Theft:<br>• Trade Secrets | "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." | Fed cases<br>DOJ |
| 2018 | Charged | Ventria | USA | Crops | Biotechnology | Threat actors—Liu | Monetary loss: >$75M | "Technology to | Fed cases<br>DOJ |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Bioscience | | Research Institute; China | | Xuejun and Sun Yue:<br>• Interstate transportat-ion<br>• Theft<br>• Conspiracy | • Development of IP: ~$75M<br><br>IP Theft:<br>• Trade Secrets<br>• Rice Technology; Rice Seeds<br><br>Theft:<br>• Physically stole rice seeds; found in luggage at Honolulu Airport | create rice seeds that contained certain proteins. These proteins could then be removed from the rice and used in medicines and pharmaceutical products."<br><br>Stole the seeds during a visit | |
| 2019 | Sentenced | Monsanto | USA | Talent Recruitment Program; PRC | Agrochemical<br><br>Biotechnology | Insider threat actor—Haitao Xiang:<br>• Conspiracy<br>• Theft<br>• FTP | IP Theft:<br>• Company's proprietary algorithm | | Fed cases<br>DOJ<br>DOJ |
| 2017 | Convicted<br><br>Acquitted | Applied Industrial Technologies | USA | Envision; China | Semiconductor | Insider threat actors—Liang Chen, Donald Olgado, Wei-Yung Hsu, and Robert Ewald:<br>• Theft<br>• Conspiracy | Monetary loss: "Millions of Dollars"<br><br>IP Theft:<br>• Downloaded information related to semiconductor wafers<br>• 16,000 drawings | To benefit a startup competing company. | Fed cases<br>DOJ<br>DG |
| 2017 | Indicted | Moody's Analytics<br><br>Siemens AG<br><br>Trimble Inc | USA<br><br>Germany | Guangzhou Bo Yu Information Technology Company Limited (AKA "Boyusec"); China | Economic Research<br><br>Financial Services<br><br>Healthcare<br><br>Power Systems<br><br>Energy Management | Cyber attack:<br>• Hacking by threat actors Wu Yingzhuo, Dong Hao and Xia Lei. | Monetary loss: "Millions of dollars"<br><br>IP Theft (combined):<br>• Private emails with proprietary and confidential economic analyses, findings, and opinions<br>• Proprietary and | | Fed cases<br>DOJ<br>DOJ |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | GPS | | commercial data<br>• Usernames and Passwords<br>• Over 400 GB of data<br>• Commercial GNSS Project<br>• Commercial business data | | |
| 2017 | Sentenced | The Chemours Company | USA | Xtrachemical; China/ Canada | Chemicals Company | Insider threat actor—Jerry Jindong Xu:<br>• Theft<br>• Conspiracy | IP Theft:<br>• Pricing information<br>• Passwords<br>• Took pictures of plant system diagrams<br>• Confidential documents | Additional activities:<br>• "Misled colleagues and fabricated assignment-s" to accumulate information<br>• Contacted potential Chinese investors to solicit funding for building a sodium cyanide plant."<br>• "Created a company, made his wife the director, and executed a non-disclosu re agreement with his co-conspirat or." | Fed cases<br>DOJ<br>DOJ |
| 2017 | Sentenced | Dura-Bar | USA | Unnamed Rival Company in China | Cast Iron Manufacturing | Insider threat actor—Robert O'Rourke:<br>• Theft<br>• Conspiracy | IP Theft:<br>• Trade secrets | After 30 years with Dura-Bar, O'Rourke stole trade secrets from them to work for a rival company in | Fed cases<br>CT<br>DOJ<br>DOJ |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | China | |
| 2017 | Sentenced | Trelleborg | USA | Taizhou CBM Future New Material Science and Technology Co. Ltd (CBMF); China<br><br>CBM International Inc., (CBMI); US Subsidiary of CBMF | Engineering<br><br>Defense<br><br>Oil and Gas<br><br>Aerospace<br><br>Underwater vehicles<br><br>Stealth Technology | Insider threat actors— Shan Shi, Uka Kalu Uche, Samuel Abotar Ogoe, Kui Bo, and Johnny Wade Randall:<br>• Conspiracy<br>• Theft<br><br>Threat actor—Hui Huang:<br>• Resided in China, tasking employees of CBMF<br><br>Venture threat—CBMF:<br>• After Shi offers to work with Trelleborg, CBMF would offer a joint venture | IP Theft:<br>• Syntactic foam | Dual-Use Technology with Military Applications | Fed cases<br>DOJ<br>DOJ<br>DOJ<br>Cool Case Example |
| 2016 | Sentenced | US Government<br><br>Department of Energy | USA | China General Nuclear Power Company (CGNPC) | Nuclear Energy<br><br>Defense<br><br>Government | Threat actor:<br>• Conspiracy<br>• Theft<br>• Recruit | Threat to national security<br><br>IP Theft:<br>• Trade secrets from recruited US-based engineers in the civil nuclear industry | “Enlisting U.S.-based nuclear experts to provide assistance in developing and producing special nuclear material in China for a Chinese state-owned nuclear power company…. without the required authorization from the U.S. Department of Energy.” | Fed cases<br>DOJ |
| 2016 | Sentenced | Unnamed Companies<br><br>US Government | USA | PRC | Military<br><br>Space | Threat actor—Tao Li:<br>• Conspiracy<br>• Illegal | US Goods to China<br><br>Threat to national security | Conspired to illegally export military- and space-grade technology from the | Fed cases<br>BIZJ<br>DOJ |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | • Exportation<br>• Wire fraud | | US to China. | |
| 2016 | Sentenced | GlaxoSmithKline (GSK) | USA | Renopharma; China | Pharmaceutical | Insider threat actors—Lucy Xi, Yan Mei, Tian Xue, and Tao Li:<br>• Theft<br>• Conspiracy | Monetary loss: ~$10B<br>• With stolen GSK data, Renopharma could be worth $10B.<br>• Each product stolen took GSK >$1B to research and develop. | | Fed cases<br>DOJ<br>DOJ<br>DOJ |
| 2015 | Sentenced | IBM Corp | USA (but Chinese branch) | Unnamed/ uncreated company; China | Software Engineering | Insider threat actor—Xu Jiaqiang:<br>• Theft<br>• Conspiracy<br>• Economic espionage | IP Theft:<br>• Source code | FBI received a report that someone in China claimed to have access to some source code and was using it for business ventures. | Fed cases<br>Reuters<br>DOJ |
| 2015 | Potential<br><br>Acquitted | Machine Zone, Inc. | USA | No company there was potential for threat | Video/ Mobile Gaming | Insider threat actor—Jing Zeng:<br>• Theft | IP Theft:<br>• Downloaded over 100 files of proprietary and confidential information, including data on user behavior | Upon Zeng's dismissal from his company, he downloaded the files. He was arrested at the airport on the way to China.<br><br>There was no transfer of information to any company; however, it could have "provide[d] valuable insight and a huge competitive advantage over other online game providers and competitors." | Fed cases<br>WSJ<br>GIB<br>DOJ |
| 2015 | Dropped | Unnamed Company<br><br>Temple University | USA | Superconduc-tor Technologies Inc.; Texas with entities | Superconduct-or | Insider threat actor—Xiaoxing Xi:<br>• Theft<br>• Wire fraud<br>• FTP; 863 | IP Theft:<br>• Technology for a pocket heater | Dismissed due to erroneous evidence | Fed cases<br>Science<br>DOJ<br>Temple<br>APS<br>OCPA |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | in China<br><br>FTP | | Program | | | |
| 2015 | Sentenced | Avago<br><br>Skyworks | USA | Uncreated / unnamed Chinese company<br><br>Tianjin University | Semiconductor | Insider threat actors—Hao Zhang and Wei Pang:<br>• Theft<br>• Conspiracy<br>• Economic Espionage | IP Theft:<br>• Trade Secrets: Surface Acoustic Waves (SAW) and Bulk Acoustic Waves (BAW) | Intended to create their own company | Fed cases<br>DOJ<br>DOJ |
| 2015 | | PPG Industries, Inc | USA | J.T.M.G. Co.; China | Glass (automotive and specialty) | Insider threat actor—Thomas Rukavina:<br>• Theft<br>• Conspiracy | IP Theft:<br>• Trade secrets<br>• Manufacturing specifications for windows utilized in high-speed transportation (ex. airplanes). | Rukavina committed suicide; however, it did not stop the investigation. | Fed cases<br>DOJ<br>CW<br>USGNN |
| 2015 | Sentenced | Small, unnamed company in Charlotte, North Carolina<br><br>Another unnamed company | USA | Unnamed Chinese Entity | USG<br><br>Energy | Insider threat actor—Xiwen Huang:<br>• Theft<br>• Conspiracy | Monetary loss: >$90M<br>• Research and development cos; Company 1: >$65M<br>• Research and development cos; Company 2: >$25M<br><br>IP Theft:<br>• Trade Secrets<br>• Confidential and proprietary information<br>• Over 500 documents<br>• Information on over 30 different products | In 2004, HUang was fired from a previous job for stealing, “proprietary and confidential information, including trade secret information and other intellectual property belonging to a Government Research Facility and two United States companies, with the intent to use the stolen information for the economic benefit of himself, a Chinese company, and others.”<br><br>He ended up stealing at least 2 unnamed U.S. companies.<br><br>Interesting story: When Huang was | Fed cases<br>DOJ<br>FBI<br>IM |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | sent to China on business for work, he dropped contact for three days; later, he disappeared from the company. In some quick Google searches, the US-based company discovered that he took all the stolen secrets to China and was pursuing business efforts there. | |
| 2014 | Sentenced | Pratt & Whitney<br><br>United Technologies Research Center | USA | | Aerospace<br><br>Government and defense | Insider threat actor—Yu Long:<br>• Theft<br>• Conspiracy | IP Theft:<br>• Trade secrets | | Fed cases<br>DOJ<br>DOJ<br>CBSNews |

Note: Many “confirmed” cases of theft by a country are denied; however, were proven by investigation.