A Survey of Reported Chinese Espionage, 2000 to the Present
March 2023

This updated survey is based on publicly available information and lists 224 reported instances of Chinese espionage directed at the United States since 2000. It does not include espionage against other countries, against U.S. firms or persons located in China, nor the many cases involving attempts to smuggle controlled items from the U.S. to China (usually munitions or controlled technologies) or the more than 1200 cases of intellectual property theft lawsuits brought by U.S. companies against Chinese entities in either the U.S. or China. The focus is on the illicit acquisition of information by Chinese intelligence officers or their agents and on the increasing number of Chinese covert influence operations.

Chinese espionage is undertaken in pursuit of China's strategic objectives. This is a change from the past where commercial motives were often equally important, but commercial espionage by both private and government entities remains a feature of Chinese spying. When Xi Jinping took office, first as Chair of the Central Military Commission in November 2012 and after he became President in March 2013, one of his first acts was to repurpose and reorient China's collection priority to better serve long -term goals, clamping down on what appeared to be collection by some PLA units intended for personal gain (i.e. stealing commercial technology and providing it to private companies for cash or favors) as part of his larger campaign against corruption. Of the 224 incidents, we found that 69% were reported after Xi took office.

We have divided the publicly know incidents into categories of military, political, and commercial espionage, and covert efforts to influence the target nation's politics. These categories are not hard and fast, since in many cases, an incident showed that Chinese collectors obtained information of both commercial and military value. A few cases reflect what seem to be global campaigns aimed at commercial, military and government targets in many countries and lasting for years.

It should be noted that the incidents of Chinese espionage far outnumber those by any other country, even Russia. The long-term cost to the American economy and national security cannot be precisely measured, but estimates run into the billions of dollars for commercial and technological espionage. Chinese espionage also created immeasurable damage to national security with the theft of weapons technology, including nuclear weapons test data. In the last few years, China has added the theft of massive quantities of personal information (PII), political coercion, and influence operations, to its espionage activities.

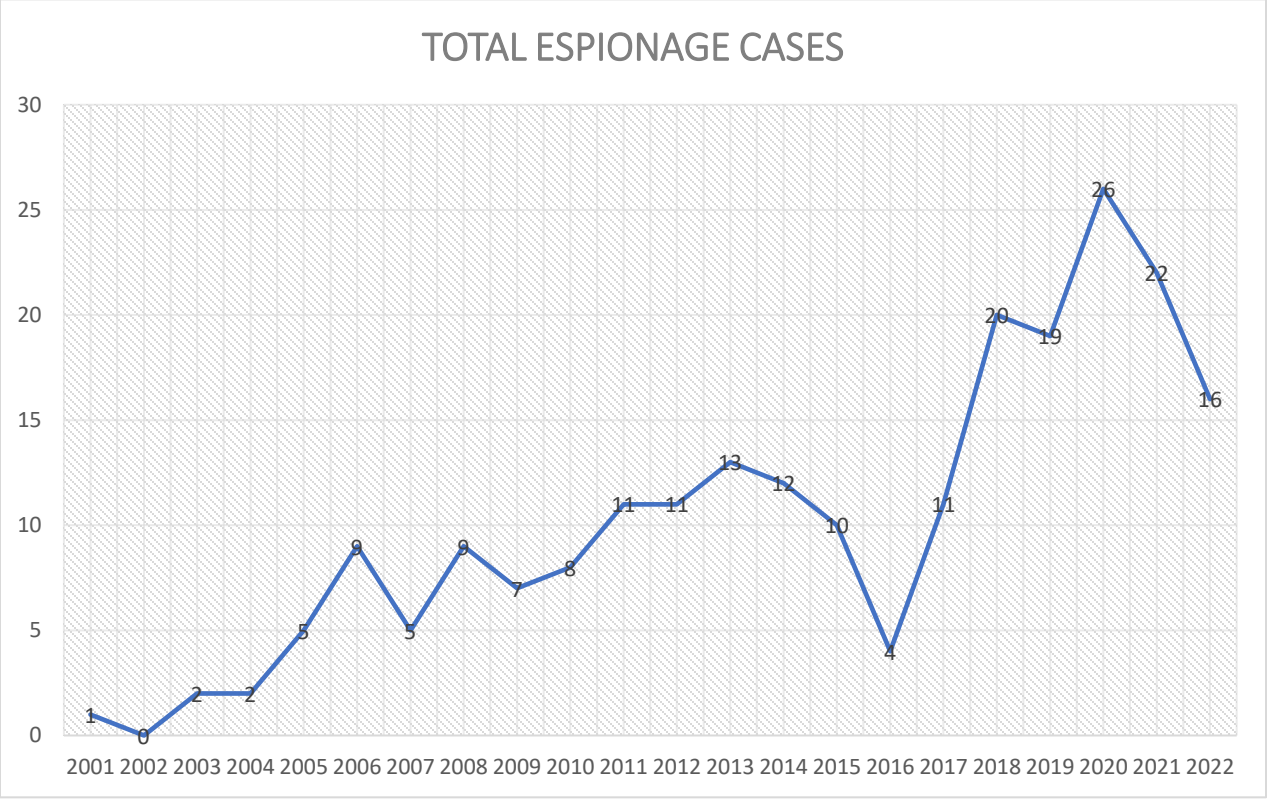
It is worth noting that while nationality is a predictive factor for espionage, ethnicity is not. Chinese nationals who come to the US to work or study are a fertile ground for recruitment. Often they intend to return to China or have close family members resident in China, making them more susceptible to coercion. In contrast, Americans of Chinese descent are very unlikely to be recruited.

The espionage problem is the result of the increasingly hostile policies of China's ruling Communist Party. Hacking is China's preferred mode of espionage. We found so many instances of reported Chinese cyber espionage – 104 in the last ten years – that we created a

separate list (Appendix A). But hacking is not the only form of spying and China uses traditional methods of agent recruitment (usually sex or money) as well as unconventional approaches, such as buying property next to a military or research facility. While this list is not complete, certain patterns emerge. For those cases where we could identify the actor and intent, we found:

- 49% of incident directly involved Chinese military or government employees.
- 41% were private Chinese citizens.
- 10% were non-Chinese actors (usually U.S. persons recruited by Chinese officials)
- 46% of incidents involved cyber espionage, usually by State-affiliated actors.
- 29% of incidents sought to acquire military technology.
- 54% of incidents sought to acquire commercial technologies.
- 17% of incidents sought to acquire information on U.S. civilian agencies or politicians.

The Chart below shows the number of publicly reported Chinese espionage incidents over time. Perhaps the most interesting part of this chart is the sharp dip after the 2015 agreement between President Obama and President Xi to restrict commercial espionage by government entities. The decline was quickly reversed within a year of the agreement.



This list is derived from open-source material and likely does not reflect the full number of incidents. It is most likely incomplete and more anecdotal than we would like. As with any list based on publicly availed information, increased numbers of incidents could reflect an increase in activity after 2009 or it could reflect increased public reporting of espionage cases, as greater attention was paid to the problem and the U.S. government became less reluctant (at the end of the Bush Administration) to publicly identify China as the perpetrator. Since these are only

reported cases, and given the clandestine nature of espionage, it is likely that this underestimates the actual scope of the problem. The list of individual incidents follows below.[1]

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.[1]

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.[2]

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]

April 2005: Chinese hackers infiltrated NASA networks managed by Lockheed Martin and Boeing and exfiltrated information about the Space Shuttle Discovery program.[6]

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.[7]

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.[8]

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.[9]

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.[10]

April 2006: Chinese hackers infiltrated NASA networks managed by Lockheed Martin and Boeing and exfiltrated information about the Space Shuttle Discovery program.[11]

---

[1] We would like to thank Shawn Rostker, Evan Burke, Matthew Serrone, Khristal Thomas, Arthur Nelson, Ian Haimowitz, David Robusto, Janice Li and Harini V for their contributions to this timeline.

May 2006: Shanshan Du stole trade secret information from General Motors for the benefit of a Chinese competitor, Chery Automobile.[12]

June 2006: Lan Lee and Yufei Ge conspired to steal trade secrets related to computer chip design and development from NetLogics Microsystems and TSMC.[13]

July 2006: Chinese hackers infiltrated the U.S. State Department's unclassified network and stole sensitive information and passwords.[14]

August 2006: Chinese hackers infiltrated the Department of Defense's non-classified NIPRNet, downloading 10 to 20 terabytes of data.[15]

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.[16]

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.[17]

December 2006: Xiang Dong Yu stole trade secret information worth $50-100 million from Ford Motor Company for the benefit of Beijing Automotive Company.[18]

December 2006: Chinese hackers infiltrated the U.S. Naval War College.[19]

2007: Chinese hackers breached the Pentagon's Joint Strike Fighter project and stole data related to the F-35 fighter jet.[20]

January 2007: The National Defense University discovered Chinese malware in its computer systems.[21]

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.[22]

September 2007: Hackers gained access to the Department of Homeland Security's networks through a contractor and exfiltrated unclassified information to Chinese servers.[23]

December 2007: Chinese hackers successfully stole information from Oak Ridge National Laboratory, Los Alamos National Laboratory, and the National Nuclear Security Administration.[24]

January 2008: Qinggui Zeng stole trade secret information related to the paint industry from an American firm for the benefit of a Chinese firm.[25]

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.[26]

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.[27]

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.[28]

May 2008: Chinese officials inserted spyware onto the laptop of U.S. Secretary of Commerce Carlos Gutierrez during a trade mission.[29]

September 2008: Anne Lockwood and Fuping Liu stole trade secret information from Metaldyne to benefit a Chinese competitor, Huafu.[30]

November 2008: Chinese hackers infiltrated the computer networks of three major oil companies and stole trade secret information.[31]

November 2008: Chinese hackers infiltrated the networks of Barack Obama and John McCain's presidential campaigns and exfiltrated information about future policy agendas.[32]

November 2008: Chinese hackers infiltrated the computer network of the White House and obtained emails between senior government officials.[33]

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.[34]

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.[35]

March 2009: Chinese hackers stole information from the Office of Senator Bill Nelson in Florida.[36]

March 2009: A Chinese espionage network was discovered to have penetrated political, economic, and social institutions in 103 countries. The network was discovered during a 10-month investigation by researchers at InfoWar Monitor when they were called to investigate the compromise of the Dalai Lama's computer systems.[37]

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.[38]

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. Meng was convicted in 2010.[39]

November 2009: Janice Capener, a Chinese national, stole trade secret information from Orbit Irrigation for the benefit of a competing Chinese firm.[40]

January 2010: Google announced that a sophisticated attack had penetrated its networks, along with the networks of more than 30 other US companies. The goal of the penetrations, which Google ascribed to China, was to collect technology, gain access to activist Gmail accounts and to Google's Gaea password management system.[41]

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.[42]

March 2010: NATO and the EU warned that the number of cyberattacks against their networks had increased significantly over the past 12 months, with Russia and China among the most active adversaries.[43]

May 2010: Glenn Shriver attempted to gain access to classified national defense information on behalf of Chinese intelligence officers.[44]

May 2010: Chinese hackers breached the computer network of the U.S. Chamber of Commerce and stole information related to U.S. industries.[45]

August 2010: Kexue Huang, a Chinese research scientist, stole trade secret information related to organic pesticides for the benefit of a Chinese firm.[46]

October 2010: York Yuan Chang and Leping Huang owned a company called General Technology Systems Integration, Inc. (GTSI), which was involved in the export of technology to the PRC. GTSI allegedly entered into contracts with the 24th Research Institute of the China Electronics Technology Corporation Group to design and transfer to the PRC technology for the development of two types of high-performance analog-to-digital converters.[47]

November 2010: Zhiqiang Zhang allegedly stole trade secret information from SiRF for the benefit of a competing Chinese firm.[48]

January 2011: A Chinese company, Pangang Group, and Walter Liew attempted to steal trade secret information related to TiO_2 technology from DuPont.[49]

February 2011: Wen Chyu Liu, a research scientist, conspired to steal trade secret information from Dow for the benefit of Chinese firms.[50]

March 2011: Sinovel, a Chinese company, stole trade secret information related to source code

and designs of superconductors from AMSC.[51]

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.[52]

April 2011: Between March 2010 and April 2011, the FBI identified twenty incidents in which the online banking credentials of small-to-medium sized U.S. businesses were compromised and used to initiate wire transfers to Chinese economic and trade companies. As of April 2011, the total attempted fraud amounts to approximately $20 million; the actual victim losses are $11 million.[53]

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. [54]

April 2011: Chinese hackers attempted to steal technical data from the computer systems of Oak Ridge National Laboratory.[55]

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.[56]

August 2011: Chinese hackers engaged in a series of cyber-attacks against 72 entities, including multiple U.S. government networks.[57]

October 2011: Chinese hackers infiltrated at least 48 chemical and defense companies and stole trade secret information and sensitive military information.[58]

November 2011: Chinese hackers interfered with U.S. satellites and stole sensitive data.[59]

February 2012: Chinese hackers stole classified information about the technologies onboard F-35 Joint Strike Fighters.[60]

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.[61]

March 2012: Trend Micro uncovered a Chinese cyber campaign, dubbed 'Luckycat' that targeted U.S.-based activists and organizations, Indian and Japanese military research, as well as Tibetan activists.[62]

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.[63]

June 2012: P.L.A. Unit 61398 attacked Digital Bond, a SCADA security company with a spear phishing attack.[64]

August 2012: Jerry Lee, a former CIA agent, attempted to provide China with classified information about CIA activities within China.[65]

September 2012: Chinese hackers infiltrated Telvent Canada, an industrial automation company, and stole data related to SCADA systems throughout North America.[66]

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.[67]

September 2012: Sixing Liu, a Chinese national, stole technical data related to defense items and conspired to give the information to China.[68]

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.[69]

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.[70]

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.[71]

January 2013: The New York Times, Wall Street Journal, Washington Post, and Bloomberg News experienced persistent cyberattacks, presumed to originate in China.[72]

February 2013: Security researchers revealed that PLA Unit 61398 had hacked 115 U.S.-victims since 2006, including organizations in the IT, aerospace, and telecommunications sectors, among others.[73]

February 2013: DHS says that between December 2011 and June 2012, cyber criminals targeted 23 gas pipeline companies and stole information that could be used for sabotage purposes. Forensic data suggests the probes originated in China.[74]

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.[75]

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.[76]

June 2013: PLA hackers infiltrated the computer networks of the U.S. Transportation Command

and stole sensitive military information.[77]

July 2013: Tung Pham stole trade secrets from a solar technology company for the benefit of a competing Chinese firm.[78]

September 2013: Chinese hackers targeted three U.S. organizations, including a large American oil and gas corporation.[79]

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.[80]

October 2013: Chinese hackers targeted a U.S. based think tank.[81]

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.[82]

December 2013: Weiqiang Zhang stole trade secret information related to rice seeds from an American agricultural firm for the benefit of a Chinese firm.[83]

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.[84]

March 2014: The OPM contractor responsible for U.S. security clearance background investigations is breached, allegedly by Chinese hackers.[85]

May 2014: Alleged Chinese hackers posed as C-Suite executives in a spear phishing campaign to access the network of Alcoa. The hackers stole 2,907 emails and 863 attachments.[86]

May 2014: Chinese military hackers targeted six American companies in the power, metals, and solar production industries and stole trade secret information. The U.S. Department of Justice indicted them and identified them as members of the People's Liberation Army Unit 61398.[87]

June 2014: Jun Xie allegedly stole trade secret information from GE Healthcare to benefit a competing entity in China.[88]

August 2014: Community Health Systems disclosed that suspected Chinese hackers infiltrated its network and stole personal information from 4.5 million patients.[89]

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.[90]

August 2014: Chinese hackers infiltrated the U.S. Investigations Services. The Office of Personnel Management discovered that China had infiltrated its networks and stolen the personal

information of federal employees, including security clearance information. This was one of the first incidents as part of the larger 2015 OPM hack.[91]

September 2014: Chinese company Huawei[92] repeatedly attempted to steal trade secret information about robotics designs from T-Mobile.[93]

September 2014: Benjamin Bishop was arrested for passing classified information between May 2012 – December 2012 to a Chinese national he was romantically involved with.[94]

November 2014: Chinese hackers breached the U.S. Postal Service computer networks and exfiltrated data of approximately 800,000 employees.[95]

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.[96]

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.[97]

February 2015: Xudong Yao stole trade secret information relating to locomotives for the benefit of a Chinese firm.[98]

March 2015: Canadian researchers say Chinese hackers launched a DDoS attack against 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. [99]

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.[100]

May 2015: Beginning in 2014, Thomas Rukavina stole and passed on trade secret information from PPG to a competing Chinese firm.[101]

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.[102]

May 2015: Chinese hackers exfiltrated significant amounts of customer data from United Airlines.[103]

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.[104]

November 2015: Dutch security firm Fox-IT identified a Chinese threat actor, 'Mofang', that had launched cyber-attacks against government civilian and military agencies in the United States and other industries, including corporations conducting solar cell research.[105]

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.[106]

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.[107]

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.[108]

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.[109]

April 2016: U.S. Steel accused Chinese government hackers of stealing proprietary information about steel production techniques for the benefit of Chinese steel producers.[110]

March 2017: A State Department employee with TS clearance provided copies of internal Department of State documents to Chinese intelligence officers.[111]

April 2017: Cybersecurity researchers revealed a growing cyber-espionage campaign originating in China and targeting construction, engineering, aerospace and telecom companies, as well as government agencies, in the U.S., Europe, and Japan.[112]

April 2017: CrowdStrike observed a China-based adversary target a U.S.-based think tank. CrowdStrike later named the adversary "Mustang Panda."[113]

May 2017: Beginning in 2011, Hackers from the internet security firm Boyusec (which has ties to MSS) 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.[114]

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.[115]

June 2017: Kevin Patrick Mallory, a former CIA officer, transferred classified documents to an agent of China's intelligence services.[116]

August 2017: Dong Liu attempted to obtain trade secret information from Medrobotics Corporation for China.[117]

September 2017: China allegedly inserted malware into a widely used PC management tool. The malware targeted at least 20 major international technology firms.[118]

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.[119]

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.[120]

November 2017: Three Chinese nationals employed at a China-based Internet security firm were indicted by a US grand jury for computer hacking, theft of trade secrets, conspiracy, and identity theft against employees of Siemens, Moody's Analytics, and Trimble.[121]

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.[122]

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.[123]

March 2018: Chinese hackers targeted U.S. defense and engineering companies with ties to the South China Sea. The attacks sought sensitive data in line with government espionage objectives.[124]

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.[125]

April 2018: A cyber espionage campaign originating in China collected data from satellite, telecom, and defense organizations in the United States and Southeast Asia.[126]

June 2018: Ron Rockwell Hansen, a former DIA officer, attempted to transmit national defense information to China.[127]

June 2018: Chinese hackers were found to be engaged in a cyber espionage campaign to collect data from satellite, telecom, and defense organizations in the U.S. and Southeast Asia.[128]

July 2018: Xiaqing Zhang conspired to steal trade secret information from General Electric for

the benefit of China.[129]

July 2018: Xiaolang Zhang was arrested for stealing trade secret information about the circuit board of Apple's self-driving car initiative. [130]

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.[131]

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.[132]

October 2018: The U.S. Department of Justice indicted Chinese intelligence officers and hackers working for them for engaging in a campaign to hack into U.S. aerospace companies and steal information.[133]

October 2018: U.S. agencies warned President Trump that that China and Russia eavesdropped on calls he made from an unsecured phone.[134]

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.[135]

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.[136]

December 2018: U.S. Navy officials report that Chinese hackers had repeatedly stolen information from Navy contractors including ship maintenance data and missile plans.[137]

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.[138]

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.[139]

December 2018: The United States, in coordination with Australia, Canada, the UK, and New Zealand, accused China of conducting a 12-year campaign of cyber espionage targeting the IP and trade secrets of companies across 12 countries. The announcement was tied to the indictment of two Chinese hackers associated with the campaign.[140]

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.[141]

January 2019: A Chinese national, Jizhong Chen, stole trade secret information about autonomous vehicles from Apple to benefit a competing Chinese firm**.**[142]

February 2019: The UN International Civil Aviation Organizations revealed that in late 2016 it was compromised by China-linked hackers who used their access to spread malware to foreign government websites.[143]

March 2019: Beginning in April 2017, Chinese hackers stole research from universities about maritime technology being developed for military use.[144]

March 2019: Chinese hackers targeted Israeli defense firms that had connections to the U.S. military.[145]

April 2019: Chinese hackers stole General Electric's trade secrets concerning jet engine turbine technologies.[146]

April 2019: Pharmaceutical company Bayer announced it had prevented an attack by Chinese hackers targeting sensitive intellectual property.[147]

May 2019: Hackers affiliated with the Chinese intelligence service reportedly had been using NSA hacking tools since 2016, more than a year before those tools were publicly leaked.[148]

June 2019: Haoyang Yu was arrested in connection with stealing proprietary information from Analog Devices, a U.S. semiconductor company. [149]

June 2019: Since at least 2017, Chinese hackers exfiltrated Call Detail Records (CDRs) from telecommunication companies to track dissidents, officials, and suspected spies.[150]

July 2019: Chinese hackers from the group APT10 targeted three U.S. utility companies with a spear-phishing campaign to gain access to computer networks.[151]

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.[152]

August 2019: Chinese state-sponsored hackers were revealed to have targeted multiple U.S. cancer institutes to take information relating to cutting edge cancer research.[153]

September 2019: Two Chinese nationals stole sensitive exosome medical research from the Nationwide Children's Hospital.[154]

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.[155] [156]

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. [157]

September 2019: A Chinese state-sponsored hacking group responsible for attacks against three U.S. utility companies in July 2019 was found to have subsequently targeted seventeen others.[158]

October 2019: Chinese hackers engaged in a multi-year campaign between 2010 and 2015 to acquire intellectual property from foreign companies to support the development of the Chinese C919 airliner.[159]

November 2019: Jerry Chun Shing Lee, a former CIA officer, was sentenced for providing classified information to Chinese intelligence officers.[160]

December 2019: An alleged Chinese state-sponsored hacking group attacked government entities and managed service providers by bypassing the two-factor authentication used by their targets.[161]

January 2020: A Harvard University Professor 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.[162]

February 2020: The U.S. Department of Justice indicted two Chinese nationals for laundering cryptocurrency for North Korean hackers.[163]

March 2020: Chinese hackers targeted over 75 organizations around the world in the manufacturing, media, healthcare, and nonprofit sectors as part of a broad-ranging cyber espionage campaign.[164]

April 2020: U.S. officials reported seeing a surge of attacks by Chinese hackers against healthcare providers, pharmaceutical manufacturers, and the U.S. Department of Health and Human services amidst the COVID-19 pandemic.[165]

May 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.[166]

May 2020: U.S. officials accused hackers linked to the Chinese government of attempting to steal U.S. research into a coronavirus vaccine.[167]

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.[168]

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.[169]

July 2020: Jun 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 and MSS.[170]

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.[171]

July 2020: Li Xiaoyu and Dong Jiazhi, two Chinese nationals, were charged by the FBI for hacking the U.S. Department of Energy on behalf of the MSS. The two allegedly had committed economic espionage, extortion, computer fraud, and IP theft over the course of 11 years.[172]

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. [173]

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. [174]

August 2020: Former CIA officer Alexander Yuk Ching Ma was arrested and charged with espionage on behalf of China's MSS. Between 2001 and 2010, Ma routinely exfiltrated classified CIA and FBI information to MSS operatives.[175]

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. [176]

September 2020: The U.S. Department of Justice charged 7 Chinese hackers with breaching more than 100 companies, think tanks, universities and government agencies around the world.[177]

September 2020: CISA revealed that hackers associated with the Chinese Ministry of State Security had been scanning U.S. government and private networks for over a year in search of

networking devices that could be compromised using exploits for recently discovered vulnerabilities.[178]

October 2020: The NSA warned that Chinese government hackers were targeting the U.S. defense industrial base as part of a wide-ranging espionage campaign.[179]

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.[180]

October 2020: Eight individuals were charged with conspiring to act as illegal agents on behalf of the PRC. The individuals engaging in "Operation Fox Hunt" allegedly attempted to harass, stalk, and coerce individuals living in the U.S. who are wanted in China to return to the country.[181]

October 2020: U.S. citizen Elliott Broidy pleaded guilty to undisclosed lobbying on behalf of the PRC in exchange for millions of dollars. Broidy attempted to get the U.S. government to drop a large fraud and money laundering prosecution and deport a critic of the PRC.[182]

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.[183]

November 2020: In 2020, two apps were banned from the Google Play Store after cybersecurity researchers discovered that a software development kit developed by the Chinese internet giant Baidu had sent sensitive data on hundreds of millions of users to Chinese servers.[184]

December 2020: Axios reported on a Chinese intelligence operation that allegedly occurred between 2011 and 2015. During the operation, a suspected Chinese spy named Fang Fang targeted local and national politicians through networking, campaign fundraising, and romantic or sexual relationships to gain proximity to political power.[185]

December 2020: Yu Zhou and his wife Li Chen admit to conspiring to steal trade secrets from the local Ohio pediatric research institute where they worked and sell them to China.[186]

January 2021: Hackers linked to the Chinese government were responsible for ransomware attacks against five major gaming and gambling countries, demanding over $100 million in ransom.[187]

January 2021: A senior NASA official was sentenced for making false statements regarding his association to the Chinese Thousand Talents Program. He lied to investigators when questioned about his membership and professorship status in universities in China.[188]

February 2021: Former University of Florida professor Lin Yang was indicted on charges to commit wire fraud and making false statements regarding a $1.75 million grant from the National Institutes of Health (NIH). The indictment alleges Yang concealed a business he established in China promoting a product he created using the NIH grant and applying to join China's Thousand Talent Program.[189]

February 2021: Visiting Stanford researcher, Chen Song was indicted for obstruction, alteration of records, visa fraud charges and false statements regarding about her status as a member of the PRC military forces while conducting brain disease research in the United States.[190]

February 2021: Hong Kong based and Chinese national, Chi Lung Winsman, was charged with conspiring to steal trade secrets from General Electric (GE). Mr. Winsman recruited a GE engineered to steal MOSFET trade secrets and other proprietary information from GE to a new venture in China.[191]

March 2021: Chinese government hackers targeted Microsoft's enterprise email software to steal data from over 30,000 organizations around the world, including government agencies, legislative bodies, law firms, defense contractors, infectious disease researchers, and policy think tanks.[192]

April 2021: Two state-backed hacking groups—one of which works on behalf of the Chinese government—exploited vulnerabilities in a VPN service to target organizations across the U.S. and Europe with a particular focus on U.S. defense contractors.[193]

April 2021: New York City's Metropolitan Transportation Authority (MTA) was hacked by Chinese-backed actors but were unable to gain access to user data or information systems.[194]

April 2021: Chinese national Suren Qin pleaded guilty to illegally exporting $100,000 of U.S. goods to PLA-affiliated Northwester Polytechnical University in China. Qin primarily sent underwater and marine technologies to the PRC through their company LinkOcean Technologies, LTD.[195]

June 2021: Chinese actors targeted organizations, including Verizon and the Metropolitan Water District of Southern California using a platform used by numerous government agencies and companies for secure remote access to their networks.[196]

July 2021: The FBI and the U.S. Cybersecurity and Infrastructure Security Agency (CISA) released a statement exposing a spearfishing campaign by Chinese state-sponsored hackers between 2011 and 2013. The campaign targeted oil and natural gas pipeline companies in the United States.[197]

July 2021: The U.S., NATO, and allies accused the PRC of using contract hackers to conduct an ongoing global cyberespionage campaign that includes ransomware attacks, cyber extortion, crypto-jacking, and theft. Accompanying this accusation were charges against four MSS hackers for engaging in a multi-year campaign to steal trade secrets, business information, IP, and Ebola vaccine research. Finally, the U.S. government announced they are attributing a March 2021 exploitation of zero-day vulnerabilities in Microsoft Exchange Server to MSS hackers.[198]

July 2021: Four Chinese hackers were indicted for a cyber operation between 2011-2018 to steal intellectual property from companies, academia and government entities in the U.S. and abroad.

The theft focused on information of significant economic benefit to Chinese state-owned enterprises.[199]

October 2021: Former U.S military pilot, Shapour Moinian, was charged with making false statements regarding his contact with Chinese intelligence including cash payments. Mr. Moinian worked for various defense contractors and traveled oversees to brief his contacts on the status of his work.[200]

October 2021: Former Air War College professor Xiaoming Zhang pleaded guilty to making false statements regarding his relationship with a known official working with the Shanghai Municipal Government. The Chinese official was attempting to leverage their relationship to gain access to sensitive relationship or other valuable individuals to the Chinese government.[201]

October 2021: A Chinese-linked hacking group gained access to calling records and text messages from telecommunication carriers across the globe, according to a report from CrowdStrike. The report outlines the group began its cyberattacks in 2016 and infiltrated at least 13 telecommunications networks.[202]

November 2021: Former Broadcom employee Peter Kisang Kim was charged with theft of trade secrets prior to his start as a director for a Chinese based start-up microprocessor company. Specifically, the indictment alleges that Kim stole trade secrets of microchip design used in high-volume data centers.[203]

November 2021: A federal jury convicted Yanjun Xu, a Chinese national and Deputy Division Director of the Sixth Bureau of the Jiangsu Province Ministry of State Security, of conspiring and attempting to commit economic espionage and theft of trade secrets. The defendant is the first Chinese intelligence officer to be extradited to the United States to stand trial.[204]

November 2021: After CISA publicly shared details on a vulnerability, Chinese hackers targeted nine companies and 370 servers between September and October using the same vulnerability.[205]

December 2021: Former U.S. Navy Sailor, Ye Sang, was sentenced for conspiring to illegally export sensitive military equipment to China. Sang purchased military equipment for Naval Special Warfare units as a logistics specialist from 2015 to 2019 and colluded with her husband to export equipment to China.[206]

December 2021: Chinese hackers breached four more U.S. defense and technology firms in December, in addition to one organization in November. The hackers obtained passwords to gain access to the organizations' systems and looked to intercept sensitive communications.[207]

December 2021: Cybersecurity firms found government-linked hackers from China, Iran, and North Korea attempting to use the Log4j vulnerability to gain access to computer networks. Following the announcement of Log4j, researchers already found over 600,000 attempts to exploit the vulnerability.[208]

January 2022: Chinese national and imaging scientist, Xiang Haitao pleaded guilty to conspiracy to commit economic espionage against Monsanto and The Climate Corporation based in St. Louis. Xiang developed a digital online farming software used to collect, store, and visualize critical agricultural field data to improve productivity, he's guilty of stealing a predictive algorithm and providing it to the Chinese Academy of Science's Institute of Soil Science.[209]

January 2022: University of Arkansas Professor, Simon Saw-Teong Ang, pleaded guilty to making a materially false and fictious statement and representation to an FBI Special Agent for failing to disclose his 24 Chinese patents to the university and to the FBI, when interviewed.[210]

February 2022: China-based Hytera Communications Corp. LTD. was indicted for conspiring with former Motorola Solutions employees to steal digital mobile radio technology developed by Motorola. The indictment alleges that from 2007 to 2020, Hytera and the recruited employees used Motorola's proprietary and trade secret information to accelerate the development of Hytera's DMR products, train Hytera employees, and market and sell Hytera's DMR products throughout the world.[211]

February 2022: An investigation led by Mandiant discovered that hackers linked to the Chinese-government compromised email accounts belonging to Wall Street Journal journalists. The hackers allegedly surveilled and exfiltrated data from the newspaper for over two years beginning in at least February 2020.[212]

March 2022: Five individuals with ties to the secret police of the People's Republic of China were charged with various crimes related to the PRC's efforts to stalk, harass and spy on Chinese nationals residing in the United States. All five perpetrated transnational repression schemes targeting U.S. residents whose political views and actions are viewed as unfavorable by the PRC, including advocacy for democracy and dissidence of the regime.[213]

March 2022: Hackers linked to the Chinese government penetrated the networks belonging to government agencies of at least 6 different U.S. states in an espionage operation. Hackers took advantage of the Log4j vulnerability to access the networks, in addition to several other vulnerable internet-facing web applications.[214]

May 2022: Wang Shujun, a U.S. citizen who helped start a pro-democracy organization in Queens opposing the current communist regime in China, was charged alongside four officials from China's Ministry of State Security (MSS) with conspiracy and other charges related to an espionage and transnational repression scheme. Wang used his position within the organization and dissident communities to collect information about prominent activists and human rights leaders for the MSS and PRC. He was handled by four MSS officials: Feng He, Jie Ji, Ming Li, and Keqing Lu.[215]

May 2022: Chenyan Wu and Lianchun Chen, a married couple who worked as research scientists for a major American pharmaceutical company, pleaded guilty in federal court to criminal charges stemming from their efforts to gather confidential mRNA research from that company to advance the husband's competing laboratory research in China.[216]

May 2022: A Chinese hacking group stole intellectual property assets from U.S and European companies since 2019 and went largely undetected. Researchers believe the group is backed by the Chinese government.[217]

June 2022: The FBI, National Security Agency (NSA) and CISA announced that Chinese state-sponsored hackers targeted and breached major telecommunications companies and network service providers since at least 2020.[218]

September 2022: A federal jury in Chicago convicted Chinese national Ji Chaoqun of acting illegally within the United States as an agent of the People's Republic of China. He was found guilty on one count of conspiracy to act as an agent of the PRC without first notifying the Attorney General; one count of acting as an agent of the PRC without first notifying the Attorney General; and one count of making a materially false statement to the U.S. Army.[219]

September 2022: Peter Kisang Kim, a former Broadcom Inc. engineer, was sentenced to eight months in prison for trade secret theft involving Broadcom trade secrets. Kim had been employed by Broadcom for over twenty years. He was indicted in November 2021 and pleaded guilty on May 10, 2022.[220]

October 2022: Two Chinese citizens were charged in a criminal complaint in federal court in New York with obstruction of justice and accused of attempting to pay bribes for inside information about the high-profile prosecution of Chinese telecommunications giant Huawei.[221]

November 2022: Suspected Chinese-linked hackers carried out an espionage campaign on public and private organizations in the Philippines, Europe, and the United States since 2021. The attacks used infected USB drives to deliver malware to the organizations.[222]

October 2022: In three separate cases in the U.S. Attorneys' Offices for the Eastern District of New York and the District of New Jersey, the Justice Department has charged 13 individuals, including members of the People's Republic of China (PRC) security and intelligence apparatus and their agents, for alleged efforts to unlawfully exert influence in the United States for the benefit of the government of the PRC.[223]

December 2022: Chinese government-linked hackers stole at least $20 million in COVID-19 relief funds from the U.S. government, including Small Business Administration loans and unemployment insurance money. The U.S. Secret Service announced they retrieved half of the stolen funds thus far.[224]

February 2023: The United States shot down a Chinese spy balloon it entered U.S. airspace near the Aleutian Islands. The balloon traversed Alaska, Canada and re-entered U.S. airspace over Idaho before travelling across the continental United States. Defense Secretary Lloyd Austin stated that the balloon "was being used by the PRC in an attempt to surveil strategic sites."[225]

Appendix A – Major Cyber Espionage Incidents Attributed to China

December 2022. Chinese government-linked hackers stole at least $20 million in COVID-19 relief funds from the U.S. government, including Small Business Administration loans and unemployment insurance money. The U.S. Secret Service announced they retrieved half of the stolen funds thus far.

November 2022. Suspected Chinese-linked hackers carried out an espionage campaign on public and private organizations in the Philippines, Europe, and the United States since 2021. The attacks used infected USB drives to deliver malware to the organizations.

June 2022. The FBI, National Security Agency (NSA) and CISA announced that Chinese state-sponsored hackers targeted and breached major telecommunications companies and network service providers since at least 2020.

May 2022. A Chinese hacking group stole intellectual property assets from U.S and European companies since 2019 and went largely undetected. Researchers believe the group is backed by the Chinese government.

March 2022. Hackers linked to the Chinese government penetrated the networks belonging to government agencies of at least 6 different U.S. states in an espionage operation. Hackers took advantage of the Log4j vulnerability to access the networks, in addition to several other vulnerable internet-facing web applications.

February 2022. An investigation led by Mandiant discovered that hackers linked to the Chinese-government compromised email accounts belonging to Wall Street Journal journalists. The hackers allegedly surveilled and exfiltrated data from the newspaper for over two years beginning in at least February 2020.

December 2021. Chinese hackers breached four more U.S. defense and technology firms in December, in addition to one organization in November. The hackers obtained passwords to gain access to the organizations' systems and looked to intercept sensitive communications.

December 2021. Cybersecurity firms found government-linked hackers from China, Iran, and North Korea attempting to use the Log4j vulnerability to gain access to computer networks. Following the announcement of Log4j, researchers already found over 600,000 attempts to exploit the vulnerability.

November 2021. After CISA publicly shared details on a vulnerability, Chinese hackers targeted nine companies and 370 servers between September and October using the same vulnerability.

October 2021. A Chinese-linked hacking group gained access to calling records and text messages from telecommunication carriers across the globe, according to a report from CrowdStrike. The report outlines the group began its cyberattacks in 2016 and infiltrated at least 13 telecommunications networks.

July 2021. Four Chinese nationals targeted companies, universities, and government entities in

the United States and abroad between 2011 and 2018. The campaign focused on information of economic benefit to China's commercial sectors.

July 2021. The United States, the European Union, NATO and other world powers released joint statements condemning the Chinese government for a series of malicious cyber activities. They attributed responsibility to China for the Microsoft Exchange hack from early 2021 and the compromise of more than 100,000 servers worldwide.

July 2021. The FBI and the U.S. Cybersecurity and Infrastructure Security Agency (CISA) released a statement exposing a spearfishing campaign by Chinese state-sponsored hackers between 2011 and 2013. The campaign targeted oil and natural gas pipeline companies in the United States.

June 2021. Chinese actors targeted organizations, including Verizon and the Metropolitan Water District of Southern California using a platform used by numerous government agencies and companies for secure remote access to their networks.

April 2021. Two state-backed hacking groups—one of which works on behalf of the Chinese government—exploited vulnerabilities in a VPN service to target organizations across the U.S. and Europe with a particular focus on U.S. defense contractors.

April 2021. New York City's Metropolitan Transportation Authority (MTA) was hacked by Chinese-backed actors but were unable to gain access to user data or information systems.

March 2021. Chinese government hackers targeted Microsoft's enterprise email software to steal data from over 30,000 organizations around the world, including government agencies, legislative bodies, law firms, defense contractors, infectious disease researchers, and policy think tanks.

January 2021. Hackers linked to the Chinese government were responsible for ransomware attacks against five major gaming and gambling countries, demanding over $100 million in ransom.

November 2020. In 2020, two apps were banned from the Google Play Store after cybersecurity researchers discovered that a software development kit developed by the Chinese internet giant Baidu had sent sensitive data on hundreds of millions of users to Chinese servers.

October 2020. A spokesperson for China's Foreign Ministry responded to accusations that Chinese state-sponsored hackers were targeting the U.S. defense industrial base by declaring that the United States was an "empire of hacking," citing 2013 leaks about the NSA's Prism program.

October 2020. The NSA warned that Chinese government hackers were targeting the U.S. defense industrial base as part of a wide-ranging espionage campaign.

September 2020. The U.S. Department of Justice indicted five Chinese hackers with ties to Chinese intelligence services for attacks on more than 100 organizations across government, IT, social media, academia, and more.

September 2020. CISA revealed that hackers associated with the Chinese Ministry of State Security had been scanning U.S. government and private networks for over a year in search of networking devices that could be compromised using exploits for recently discovered vulnerabilities.

May 2020. U.S. officials accused hackers linked to the Chinese government of attempting to steal U.S. research into a coronavirus vaccine

April 2020. U.S. officials reported seeing a surge of attacks by Chinese hackers against healthcare providers, pharmaceutical manufacturers, and the U.S. Department of Health and Human services amidst the COVID-19 pandemic.

March 2020. Chinese hackers targeted over 75 organizations around the world in the manufacturing, media, healthcare, and nonprofit sectors as part of a broad-ranging cyber espionage campaign.

February 2020. The U.S. Department of Justice indicted two Chinese nationals for laundering cryptocurrency for North Korean hackers

December 2019. An alleged Chinese state-sponsored hacking group attacked government entities and managed service providers by bypassing the two-factor authentication used by their targets

October 2019. Chinese hackers engaged in a multi-year campaign between 2010 and 2015 to acquire intellectual property from foreign companies to support the development of the Chinese C919 airliner.

October 2019. A Chinese government-sponsored propaganda app with more than 100 million users was found to have been programmed to have a backdoor granting access to location data, messages, photos, and browsing history, as well as remotely activate audio recordings.

September 2019. A Chinese state-sponsored hacking group responsible for attacks against three U.S. utility companies in July 2019 was found to have subsequently targeted seventeen others.

August 2019. Chinese state-sponsored hackers were revealed to have targeted multiple U.S. cancer institutes to take information relating to cutting edge cancer research.

August 2019. A previously unidentified Chinese espionage group was found to have worked since 2012 to gather data from foreign firms in industries identified as strategic priorities by the Chinese government, including telecommunications, healthcare, semiconductor manufacturing, and machine learning. The group was also active in the theft of virtual currencies and the monitoring of dissidents in Hong Kong.

July 2019. State-sponsored Chinese hackers conducted a spear-phishing campaign against employees of three major U.S. utility companies

June 2019. Over the course of seven years, a Chinese espionage group hacked into ten international cellphone providers operating across thirty countries to track dissidents, officials, and suspected spies.

May 2019. Hackers affiliated with the Chinese intelligence service reportedly had been using NSA hacking tools since 2016, more than a year before those tools were publicly leaked.

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

April 2019. Pharmaceutical company Bayer announced it had prevented an attack by Chinese hackers targeting sensitive intellectual property.

March 2019. U.S. officials reported that at least 27 universities in the U.S. had been targeted by Chinese hackers as part of a campaign to steal research on naval technologies.

February 2019. The UN International Civil Aviation Organizations revealed that in late 2016 it was compromised by China-linked hackers who used their access to spread malware to foreign government websites.

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.

December 2018. The United States, in coordination with Australia, Canada, the UK, and New Zealand, accused China of conducting a 12-year campaign of cyber espionage targeting the IP and trade secrets of companies across 12 countries. The announcement was tied to the indictment of two Chinese hackers associated with the campaign.

December 2018. U.S. Navy officials report that Chinese hackers had repeatedly stolen information from Navy contractors including ship maintenance data and missile plans.

December 2018. Secretary of State Mike Pompeo confirmed that Chinese hackers breached the systems of an American hotel chain, stealing the personal information of over 500 million customers.

October 2018. U.S. agencies warned President Trump that that China and Russia eavesdropped on calls he made from an unsecured phone.

October 2018. The U.S. Department of Justice indicted Chinese intelligence officers and hackers working for them for engaging in a campaign to hack into U.S. aerospace companies and steal information

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

June 2018. Chinese hackers were found to be engaged in a cyber espionage campaign to collect data from satellite, telecom, and defense organizations in the U.S. and Southeast Asia.

June 2018. Chinese government hackers compromised the networks of a U.S. Navy contractor, stealing 614 GB of data related to weapons, sensor, and communication systems under development for U.S. submarines.

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

March 2018. Chinese hackers targeted U.S. defense and engineering companies with ties to the South China Sea. The attacks sought sensitive data in line with government espionage objectives.

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

November 2017. Three Chinese nationals employed at a China-based Internet security firm are indicted by a US grand jury for computer hacking, theft of trade secrets, conspiracy, and identity theft against employees of Siemens, Moody's Analytics, and Trimble.

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

October 2017. China allegedly carried out a cyberattack against a U.S. think tank and law firm, both involved with fugitive Chinese tycoon Guo Wengui.

April 2017. Cybersecurity researchers revealed a growing cyber-espionage campaign originating in China and targeting construction, engineering, aerospace and telecom companies, as well as government agencies, in the U.S., Europe, and Japan.

April 2016. U.S. Steel accused Chinese government hackers of stealing proprietary information about steel production techniques for the benefit of Chinese steel producers

November 2015. Dutch security firm Fox-IT identified a Chinese threat actor, 'Mofang', that had launched cyber-attacks against government civilian and military agencies in the United States and other industries, including corporations conducting solar cell research

May 2015. Chinese hackers exfiltrated significant amounts of customer data from United Airlines

March 2015. Canadian researchers say Chinese hackers attacked U.S. hosting site GitHub. GitHub said the attack involved "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 (https://en.greatfire.org/) and the New York Times' Chinese mirror site – both of which circumvent China's firewall.

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

May 2014. Alleged Chinese hackers posed as C-Suite executives in a spear phishing campaign to access the network of Alcoa. The hackers stole 2,907 emails and 863 attachments.

March 2014. The OPM contractor responsible for U.S. security clearance background investigations is breached, allegedly by Chinese hackers.

September 2013. Chinese hackers used malware, known as 'Sykipot', to target entities in the U.S. Defense Industries and companies in key industries such as: telecommunications, computer hardware, government contractors, and aerospace. In mid-2013 they targeted the U.S. civil aviation sector.

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

May 2013. Chinese hackers compromise 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.

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.

February 2013. DHS says that between December 2011 and June 2012, cyber criminals targeted 23 gas pipeline companies and stole information that could be used for sabotage purposes. Forensic data suggests the probes originated in China.

January 2013. The New York Times, Wall Street Journal, Washington Post, and Bloomberg News experience persistent cyberattacks, presumed to originate in China.

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

September 2012. Chinese hackers infiltrated Telvent Canada, an industrial automation company, and stole data related to SCADA systems throughout North America.

June 2012. DHS reported that between December 2011 and June 2012, hackers targeted 23 gas pipeline companies and stole information that could be used for sabotage purposes. Forensic data suggests the probes originated in China.

March 2012. Trend Micro uncovered a Chinese cyber campaign, dubbed 'Luckycat' that targeted U.S.-based activists and organizations, Indian and Japanese military research, as well as Tibetan activists.

March 2012. NASA's Inspector General reported that 13 APT attacks successfully compromised 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 Joint Propulsion Laboratory involving China-based IP let the intruders gain full access to key JPL systems and sensitive user accounts.

February 2012. Media reports say that Chinese hackers stole classified information about the technologies onboard F-35 Joint Strike Fighters.

November 2011. According to a major U.S. news source, Chinese hackers interfered with two satellites belonging to NASA and USGS.

October 2011. Networks of 48 companies in the chemical, defense, and other industries were penetrated for at least six months by a hacker looking for intellectual property. Some of the attacks are attributed to computers in Hebei, China.

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

April 2011. Between March 2010 and April 2011, the FBI identified twenty incidents in which the online banking credentials of small-to-medium sized U.S. businesses were compromised and used to initiate wire transfers to Chinese economic and trade companies. As of April 2011, the total attempted fraud amounts to approximately $20 million; the actual victim losses are $11 million.

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

April 2011. Google reported a phishing effort to compromise hundreds of Gmail passwords for accounts of prominent people, including senior U.S. officials. Google attributes the effort to China.

March 2010. NATO and the EU warned that the number of cyberattacks against their networks had increased significantly over the past 12 months, with Russia and China among the most active adversaries.

January 2010. Google announced that a sophisticated attack had penetrated its networks, along with the networks of more than 30 other US companies. The goal of the penetrations, which Google

ascribed to China, was to collect technology, gain access to activist Gmail accounts and to Google's Gaea password management system.

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, and Dow Chemical.

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

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.[ccxxvii]

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

March 2009: A Chinese espionage network was discovered to have penetrated political, economic, and social institutions in 103 countries. The network was discovered during a 10-month investigation by researchers at InfoWar Monitor when they were called to investigate the compromise of the Dalai Lama's computer systems.[ccxxix]

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

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

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

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

December 2007: Chinese hackers successfully stole information from Oak Ridge National

September 2007: Hackers gained access to the Department of Homeland Security's networks through a contractor and exfiltrated unclassified information to Chinese servers.[ccxxxiv]
Laboratory, Los Alamos National Laboratory, and the National Nuclear Security Administration.[ccxxxv]

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.[ccxxxvi]

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

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

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.[ccxxxix]

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

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

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

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

April 2005: Chinese hackers infiltrated NASA networks managed by Lockheed Martin and Boeing and exfiltrated information about the Space Shuttle Discovery program.[ccxliv]

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.[ccxlv]

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.[ccxlvi]

End Notes

[1] https://www.justice.gov/archive/criminal/cybercrime/press-releases/2002/lucentSupIndict.htm
[2] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[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.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[7] https://www.justice.gov/opa/pr/hawaii-man-sentenced-32-years-prison-providing-defense-information-and-services-people-s
[8] https://www.justice.gov/archive/opa/pr/2008/March/08_nsd_229.html
[9] http://www.nbcnews.com/id/12836771/ns/us_news-security/t/taiwanese-man-admits-acting-covert-agent/#.XUSUGm9KjIU
[10] https://www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html
[11] https://www.bloomberg.com/news/articles/2008-11-19/network-security-breaches-plague-nasa
[12] https://www.justice.gov/file/347376/download: https://www.cbsnews.com/news/couple-convicted-of-stealing-gm-trade-secrets
[13] https://www.justice.gov/archive/criminal/cybercrime/press-releases/2006/liIndict.htm
[14] https://www.cbsnews.com/news/state-department-computers-hacked/
[15] https://gcn.com/articles/2006/08/17/red-storm-rising.aspx
[16] https://www.justice.gov/archive/criminal/cybercrime/press-releases/2006/mengCharge.htm
[17] https://www.justice.gov/archive/criminal/cybercrime/press-releases/2006/yePlea.htm
[18] https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2012/03/15/yuPlea.pdf
[19] https://fcw.com/articles/2006/12/04/china-is-suspected-of-hacking-into-navy-site.aspx?sc_lang=en
[20] Dreazen, "Computer Spies Breach Fighter-Jet Project."
[21] https://www.washingtontimes.com/news/2007/jan/12/20070112-123024-8199r/
[22] https://www.ft.com/content/9dba9ba2-5a3b-11dc-9bcd-0000779fd2ac
[23] http://www.cnn.com/2007/US/09/24/homelandsecurity.computers/index.html
[24] http://www.nytimes.com/2007/12/09/us/nationalspecial3/09hack.html
[25] https://www.justice.gov/archive/criminal/cybercrime/press-releases/2008/zengConvict.pdf
[26] http://www.nbcnews.com/id/35300466/ns/us_news-security/t/chinese-born-engineer-gets-years-spying/
[27] https://www.nytimes.com/2008/07/10/washington/10spy.html
[28] https://www.justice.gov/archive/criminal/cybercrime/press-releases/2008/jinIndict
[29] http://www.nbcnews.com/id/24880526/ns/us_news-security/t/did-chinese-hack-cabinet-secretarys-laptop/
[30] https://www.justice.gov/archive/criminal/cybercrime/press-releases/2008/lockwoodPlea.pdf
[31] https://www.csmonitor.com/USA/2010/0125/US-oil-industry-hit-by-cyberattacks-Was-China-involved
[32] http://www.cnn.com/2008/TECH/11/06/campaign.computers.hacked/
[33] https://www.ft.com/content/2931c542-ac35-11dd-bf71-000077b07658
[34] https://www.justice.gov/nsd/files/export_case_list_june_2016_2.pdf/download
[35] https://www.bloomberg.com/news/articles/2012-11-04/coke-hacked-and-doesn-t-tell
[36] https://miamiherald.typepad.com/nakedpolitics/2009/03/nelson-gets-hacked-and-hacked-off.html
[37] https://www.telegraph.co.uk/news/worldnews/asia/china/5071124/Chinas-global-cyber-espionage-network-GhostNet-penetrates-103-countries.html
[38] https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2012/03/15/zhuIndict.pdf
[39] https://www.justice.gov/nsd/files/export_case_list_june_2016_2.pdf/download
[40] https://www.justice.gov/sites/default/files/pages/attachments/2015/07/22/export-case-list-201505-final.pdf
[41] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[42] https://www.armed-services.senate.gov/press-releases/sasc-investigation-finds-chinese-intrusions-into-key-defense-contractors
[43] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[44] https://www.justice.gov/opa/pr/michigan-man-sentenced-48-months-attempting-spy-people-s-republic-china
[45] https://www.wsj.com/articles/SB10001424052970204058404577110541568535300

[46] https://www.justice.gov/opa/pr/chinese-national-sentenced-87-months-prison-economic-espionage-and-theft-trade-secrets
[47] https://www.justice.gov/nsd/files/export_case_list_june_2016_2.pdf/download
[48] https://www.cio.com/article/2413391/man-charged-with-stealing-secrets-from-wireless-company-sirf.html
[49] https://www.justice.gov/usao-ndca/pr/four-chinese-state-owned-industrial-companies-arraigned-economic-espionage-conspiracy
[50] https://www.justice.gov/opa/pr/former-dow-research-scientist-sentenced-60-months-prison-stealing-trade-secrets-and-perjury
[51] https://www.justice.gov/opa/pr/chinese-company-sinovel-wind-group-convicted-theft-trade-secrets
[52] https://www.nytimes.com/2011/03/18/technology/18secure.html
[53] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[54] 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
[55] http://www.computerworld.com/article/2507715/cybercrime-hacking/oak-ridge-national-lab-shuts-down-internet--email-after-cyberattack.html
[56] https://www.justice.gov/nsd/files/export_case_list_june_2016_2.pdf/download
[57] https://www.reuters.com/article/us-cyberattacks/state-actor-behind-slew-of-cyber-attacks-idUSTRE7720HU20110803
[58] https://www.reuters.com/article/us-cyberattack-chemicals-idUSTRE79U4K920111031
[59]https://web.archive.org/web/20111124012100/http://www.uscc.gov/annual_report/2011/annual_report_full_11.pdf
[60] 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
[61] https://www.reuters.com/article/us-nasa-cyberattack/nasa-says-was-hacked-13-times-last-year-idUSTRE8211G320120303
[62] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[63] https://www.csmonitor.com/Environment/2013/0227/Exclusive-Cyberattack-leaves-natural-gas-pipelines-vulnerable-to-sabotage
[64] https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf
[65] https://www.justice.gov/usao-edva/pr/former-cia-officer-pleads-guilty-conspiracy-commit-espionage
[66] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[67] justice.gov/usao-ndca/pr/four-executives-bay-area-semiconductor-equipment-manufacturer-charged-alleged
[68] https://www.justice.gov/usao-nj/pr/former-employee-new-jersey-defense-contractor-sentenced-70-months-prison-exporting
[69] https://www.justice.gov/usao-wdmo/pr/chinese-business-owner-employee-plead-guilty-sentenced-stealing-trade-secrets-sedalia
[70] https://www.justice.gov/usao-cdca/pr/chinese-national-who-stole-trade-secrets-while-working-medical-device-companies
[71] 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
[72] https://www.nytimes.com/2013/02/02/technology/washington-posts-joins-list-of-media-hacked-by-the-chinese.html
[73] https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf
[74] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[75] https://www.crowdstrike.com/blog/whois-anchor-panda/
[76] https://www.pcworld.com/article/2037037/us-department-of-labor-website-infected-with-malware.html
[77] https://www.armed-services.senate.gov/press-releases/sasc-investigation-finds-chinese-intrusions-into-key-defense-contractors
[78] https://www.justice.gov/usao-edpa/pr/solar-technology-research-scientist-pleas-guilty-wire-fraud
[79] https://www.theregister.co.uk/2013/09/26/icefog_hit_and_run_apt_japan_south_korea/
[80] https://blog.trendmicro.com/trendlabs-security-intelligence/sykipot-now-targeting-us-civil-aviation-sector-information/
[81] https://www.fireeye.com/blog/threat-research/2013/10/know-your-enemy-tracking-a-rapidly-evolving-apt-actor.html

[82] https://www.justice.gov/usao-sdia/pr/six-chinese-nationals-indicted-conspiring-steal-trade-secrets-us-seed-companies
[83] https://www.justice.gov/opa/page/file/1122681/download
[84] https://www.justice.gov/nsd/page/file/1044446/download
[85] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[86] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[87] https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor
[88] https://www.meddeviceonline.com/doc/ge-files-charges-against-chinese-engineer-for-stealing-trade-secrets-0001
[89] https://time.com/3148773/report-devastating-heartbleed-flaw-was-used-in-hospital-hack/
[90] https://www.justice.gov/usao-cdca/pr/los-angeles-grand-jury-indicts-chinese-national-computer-hacking-scheme-allegedly
[91] 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
[92] Earlier reporting on credible allegations of Huawei's theft of technology from the Canadian company Nortel are not included despite Nortel having a strong presence in the US.
[93] https://www.justice.gov/opa/press-release/file/1124996/download
[94] https://www.reuters.com/article/usa-china-espionage-idUSL1N0RJ02T20140918
[95] https://www.w ashingtonpost.com/news/federal-eye/wp/2014/11/10/china-suspected-of-breaching-u-s-postal-service-computer-networks/
[96] https://www.justice.gov/opa/pr/chinese-national-admits-stealing-sensitive-military-program-documents-united-technologies
[97] https://www.justice.gov/opa/pr/member-sophisticated-china -hacking-group-indicted-series-computer-intrusions-including
[98] https://www.justice.gov/opa/pr/newly-unsealed-federal-indictment-charges-software-engineer-taking-stolen-trade-secrets-china
[99] https://www.theguardian.com/technology/2015/mar/30/github-cleans-up-cyber-attack
[100] https://www.justice.gov/usao-wdnc/pr/chinese-businessman-charged-theft-trade-secrets
[101] https://www.justice.gov/usao-wdpa/pr/former-ppg-employee-charged-theft-trade-secrets
[102] https://www.justice.gov/opa/pr/chinese-professors-among-six-defendants-charged-economic-espionage-and-theft-trade-secrets
[103] https://www.bloomberg.com/news/articles/2015-07-29/china-tied-hackers-that-hit-u-s-said-to-breach-united-airlines
[104] https://www.justice.gov/usao-ndil/pr/businessman-indicted-allegedly-stealing-employer-s-trade-secrets-while-planning-new-job
[105] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[106] https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-economic-espionage-charges-against-chinese-man-stealing
[107] https://www.justice.gov/usao-edpa/pr/second-former-glaxosmithkline-scientist-pleads-guilty-stealing-trade-secrets-benefit
[108] https://www.justice.gov/usao-sdny/pr/former-fbi-employee-sentenced-manhattan-federal-court-24-months-prison-acting-agent
[109] https://www.justice.gov/nsd/page/file/1044446/download
[110] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[111] https://www.apnews.com/957fced045b1624d5e3d46cba250125e
[112] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[113] https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-june-mustang-panda/
[114] https://www.justice.gov/opa/pr/former-state-department-employee-sentenced-conspiring-chinese-agents
[115] https://www.justice.gov/opa/page/file/1122681/download
[116] https://www.justice.gov/opa/page/file/1122681/download
[117] https://www.justice.gov/usao-ma/pr/dual-canadianchinese-citizen-arrested-attempting-steal-trade-secrets-and-computer
[118] https://blog.checkpoint.com/2017/06/01/fireball-chinese-malware-250-million-infection/
[119] https://www.wsj.com/articles/chinese-governments-battle-against-fugitive-guo-wengui-spills-into-washington-1507260255

[120] https://www.justice.gov/usao-de/pr/former-chemours-employee-charged-conspiracy-steal-trade-secrets-connection-plan-sell
[121] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[122] https://www.justice.gov/opa/pr/electrical-engineer-convicted-conspiring-illegally-export-china-semiconductor-chips-missile
[123] https://www.reuters.com/article/us-usa-china-cyber/china-hacked-sensitive-us-navy-undersea-warfare-plans-washington-post-idUSKCN1J42MM
[124] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[125] https://www.justice.gov/opa/page/file/1122681/download
[126] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets
[127] https://www.justice.gov/opa/pr/former-defense-intelligence-officer-pleads-guilty-attempted-espionage
[128] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[129] https://www.justice.gov/opa/pr/new-york-man-charged-theft-trade-secrets
[130] https://www.bizjournals.com/sanjose/news/2018/07/17/apple-employee-pleads-not-guilty-car-secrets-aapl.html
[131] https://www.politico.com/story/2018/12/12/pompeo-says-china-hacked-marriott-1059172
[132] https://www.justice.gov/opa/page/file/1122681/download
[133] https://www.justice.gov/opa/pr/chinese-intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal
[134] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[135] https://www.justice.gov/opa/page/file/1122681/download
[136] https://www.justice.gov/opa/press-release/file/1132356/download
[137] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[138] https://www.scmp.com/news/world/united-states-canada/article/2179192/chinese-battery-expert-hongjin-tan-charged-stealing
[139] https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion
[140] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[141] https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion
[142] https://www.scmp.com/news/china/science/article/2184393/chinese-man-jizhong-chen-stole-apples-future-car-secrets-company
[143] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[144] https://www.wsj.com/articles/chinese-hackers-target-universities-in-pursuit-of-maritime-military-secrets-11551781800
[145] 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/
[146] https://www.justice.gov/opa/pr/former-ge-engineer-and-chinese-businessman-charged-economic-espionage-and-theft-ge-s-trade
[147] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[148] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[149] https://www.justice.gov/usao-ma/pr/lexington-man-and-semiconductor-company-indicted-theft-trade-secrets
[150] https://www.wsj.com/articles/global-telecom-carriers-attacked-by-suspected-chinese-hackers-11561428003
[151] https://www.forbes.com/sites/zakdoffman/2019/08/03/chinese-state-hackers-suspected-of-malicious-cyber-attack-on-u-s-utilities/?sh=6c90a6776758
[152] 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/
[153] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[154] https://www.justice.gov/opa/pr/couple-who-worked-local-research-institute-10-years-charged-stealing-trade-secrets-wire-fraud
[155] https://www.justice.gov/opa/press-release/file/1202996/download
[156] https://www.justice.gov/opa/pr/chinese-government-employee-charged-manhattan-federal-court-participating-conspiracy
[157] https://www.justice.gov/opa/pr/former-intelligence-officer-convicted-attempted-espionage-sentenced-10-years-federal-prison
[158] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

[159] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[160] https://www.justice.gov/opa/pr/former-cia-officer-sentenced-conspiracy-commit-espionage
[161] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[162] https://www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related
[163] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[164] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[165] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[166] https://www.justice.gov/opa/pr/university-researcher-pleads-guilty-lying-grant-applications-develop-scientific-expertise
[167] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[168] https://www.justice.gov/opa/pr/chinese-citizen-convicted-economic-espionage-theft-trade-secrets-and-conspiracy
[169] https://www.justice.gov/opa/pr/researchers-charged-visa-fraud-after-lying-about-their-work-china-s-people-s-liberation-army
[170] https://www.justice.gov/opa/pr/singaporean-national-pleads-guilty-acting-united-states-illegal-agent-chinese-intelligence
[171] https://www.justice.gov/opa/pr/university-arkansas-professor-indicted-wire-fraud-and-passport-fraud
[172] https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion
[173] https://www.justice.gov/opa/pr/nasa-researcher-arrested-false-statements-and-wire-fraud-relation-china-s-talents-program
[174] https://www.justice.gov/opa/pr/chinese-national-charged-destroying-hard-drive-during-fbi-investigation-possible-transfer
[175] https://news.clearancejobs.com/2020/08/18/chinas-mss-uses-alexander-ma-to-penetrate-fbi/
[176] https://www.justice.gov/opa/pr/new-york-city-police-department-officer-charged-acting-illegal-agent-people-s-republic-china
[177] https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer
[178] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[179] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[180] https://www.justice.gov/opa/pr/chinese-energy-company-us-oil-gas-affiliate-and-chinese-national-indicted-theft-trade-secrets
[181] https://www.justice.gov/opa/pr/eight-individuals-charged-conspiring-act-illegal-agents-people-s-republic-china
[182] https://www.justice.gov/opa/pr/elliott-broidy-pleads-guilty-back-channel-lobbying-campaign-drop-1mdb-investigation-and
[183] https://www.justice.gov/opa/pr/former-raytheon-engineer-sentenced-exporting-sensitive-military-related-technology-china
[184] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[185] https://www.axios.com/china-spy-california-politicians-9d2dfb99-f839-4e00-8bd8-59dec0daf589.html
[186] https://www.justice.gov/opa/pr/man-who-worked-local-research-institute-10-years-pleads-guilty-conspiring-steal-trade-secrets
[187] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[188] https://www.justice.gov/usao-sdny/pr/senior-nasa-scientist-sentenced-prison-making-false-statements-related-chinese-thousand
[189] https://www.justice.gov/opa/pr/former-university-florida-researcher-indicted-scheme-defraud-national-institutes-health-and
[190] https://www.justice.gov/opa/pr/federal-charges-against-stanford-university-researcher-expanded
[191] https://www.justice.gov/opa/pr/chinese-businessman-charged-conspiring-steal-trade-secrets
[192] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[193] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[194] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[195] https://www.justice.gov/opa/pr/chinese-national-pleads-guilty-illegal-exports-northwestern-polytechnical-university
[196] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[197] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

[198] https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/
[199] https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion
[200] https://www.justice.gov/usao-sdca/pr/former-us-military-pilot-charged-making-false-statements-national-security-background
[201] https://www.justice.gov/opa/pr/former-air-war-college-professor-pleads-guilty-making-false-statements-about-relationship
[202] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[203] https://www.justice.gov/usao-ndca/pr/former-broadcom-engineer-charged-theft-trade-secrets
[204] https://www.justice.gov/opa/pr/jury-convicts-chinese-intelligence-officer-espionage-crimes-attempting-steal-trade-secrets
[205] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[206] https://www.justice.gov/usao-sdca/pr/former-us-navy-sailor-sentenced-25-years-selling-export-controlled-military-equipment
[207] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[208] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[209] https://www.justice.gov/opa/pr/chinese-national-pleads-guilty-economic-espionage-conspiracy
[210] https://www.justice.gov/usao-wdar/pr/university-arkansas-professor-pleads-guilty-lying-federal-agents-about-patents-china
[211] https://www.justice.gov/usao-ndil/pr/federal-indictment-charges-telecommunications-company-conspiring-former-motorola
[212] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[213] https://www.justice.gov/opa/pr/five-individuals-charged-variously-stalking-harassing-and-spying-us-residents-behalf-prc-0
[214] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[215] https://www.justice.gov/opa/pr/us-citizen-and-four-chinese-intelligence-officers-charged-spying-prominent-dissidents-human
[216] https://www.justice.gov/usao-sdca/pr/husband-and-wife-scientists-plead-guilty-illegally-importing-potentially-toxic-lab
[217] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[218] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[219] https://www.justice.gov/usao-ndil/pr/chinese-national-convicted-acting-within-united-states-unregistered-agent-people-s
[220] https://www.justice.gov/usao-ndca/pr/former-broadcom-engineer-sentenced-eight-months-prison-theft-trade-secrets
[221] https://www.justice.gov/opa/press-release/file/1546421/download
[222] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[223] https://www.justice.gov/opa/pr/two-arrested-and-13-charged-three-separate-cases-alleged-participation-malign-schemes-united
[224] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[225] https://www.defense.gov/News/News-Stories/Article/Article/3288543/f-22-safely-shoots-down-chinese-spy-balloon-off-south-carolina-coast/
[ccxxvi] https://www.justice.gov/sites/default/files/pages/attachments/2015/07/22/export-case-list-201505-final.pdf
[ccxxvii] https://www.bloomberg.com/news/articles/2012-11-04/coke-hacked-and-doesn-t-tell
[ccxxviii] https://miamiherald.typepad.com/nakedpolitics/2009/03/nelson-gets-hacked-and-hacked-off.html
[ccxxix] https://www.telegraph.co.uk/news/worldnews/asia/china/5071124/Chinas-global-cyber-espionage-network-GhostNet-penetrates-103-countries.html
[ccxxx] https://www.csmonitor.com/USA/2010/0125/US-oil-industry-hit-by-cyberattacks-Was-China-involved
[ccxxxi] http://www.cnn.com/2008/TECH/11/06/campaign.computers.hacked/
[ccxxxii] https://www.ft.com/content/2931c542-ac35-11dd-bf71-000077b07658
[ccxxxiii] http://www.nbcnews.com/id/24880526/ns/us_news-security/t/did-chinese-hack-cabinet-secretarys-laptop/
[ccxxxiv] http://www.cnn.com/2007/US/09/24/homelandsecurity.computers/index.html
[ccxxxv] http://www.nytimes.com/2007/12/09/us/nationalspecial3/09hack.html
[ccxxxvi] https://www.ft.com/content/9dba9ba2-5a3b-11dc-9bcd-0000779fd2ac
[ccxxxvii] Dreazen, “Computer Spies Breach Fighter-Jet Project.”

[ccxxxviii] https://www.washingtontimes.com/news/2007/jan/12/20070112-123024-8199r/
[ccxxxix] https://www.justice.gov/archive/criminal/cybercrime/press-releases/2006/yePlea.htm
[ccxl] https://fcw.com/articles/2006/12/04/china-is-suspected-of-hacking-into-navy-site.aspx?sc_lang=en
[ccxli] https://gcn.com/articles/2006/08/17/red-storm-rising.aspx
[ccxlii] https://www.cbsnews.com/news/state-department-computers-hacked/
[ccxliii] https://www.bloomberg.com/news/articles/2008-11-19/network-security-breaches-plague-nasa
[ccxliv] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[ccxlv] https://www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html
[ccxlvi] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents