A TYPOLOGY OF CHINA'S INTELLECTUAL PROPERTY THEFT TECHNIQUES

Glenn Chafetz

September 7, 2023

INTRODUCTION

After decades of ignoring the problem, the United States and its allies now comprehend the national security, economic, and political consequences of the torrent of intellectual property (IP) that the People's Republic of China (PRC) diverts from foreign private companies. However, democratic governments are not and can never be fully equipped to protect millions of their private firms, especially without assistance from the private sector itself. Governments spend significant resources protecting state secrets, but governments and private firms spend almost nothing protecting sensitive, valuable private sector information. Private companies still do not understand the nature, scale, variety or consequences of the commercial espionage threat. And government does little to assist them.

Large companies may spend for some degree of security, but those efforts are spotty, and focus on cyber threats and occasionally insider risk, which constitute only two of multiple vectors of IP transfer. Some companies spend significant sums on fraud detection or inventory loss prevention. However, when it comes to protecting trade secrets and other IP, individual companies devote almost no resources. Three main reasons account for this inattention.

First, IP theft is not often obvious or even detectable. IP theft is espionage, not burglary. When inventory goes missing, companies often see that it's gone. When money disappears, firms can do an accounting and eventually see that it's missing. However, when firms suffer a theft of IP, they often do not learn of the loss until months or even years after the theft, if they become aware of it at all. Perhaps thieves took time to reverse engineer the product, or encountered production problems, or decided to sell in a market where the U.S. firm does not operate.

Second, victimized companies sometimes do not care about the theft or are afraid to report or respond. Some executives are not concerned with IP losses because the corporate spies took version 2.0, and the U.S. company is on version 3.0. This attitude may make sense for the short term, but it neglects the fact that a competitor stole the IP and was able to save time and money by avoiding an entire phase of R&D. This dynamic is in effect a subsidy from the victim to its competition.

Third, even if company owners and executives know and care about IP theft, the means of prevention and recourse are unclear and challenging. For one thing, each individual company is facing not just one or two corporate spies or fraudsters, but the entire mass of a powerful, sovereign state, including its intelligence services working in conjunction with its private sector. China excels at espionage, but private companies in the U.S., the E.U., Japan, and South Korea focus on their business, not counterintelligence. In today's environment, that must change. Running a successful business now must include counterintelligence, and it starts with understanding the principal techniques of technology acquisition China employs, both singly and in combination.

Toward that end, the following typology will allow companies and their employees to gain a basic understanding of the challenge they face; to recognize and understand different methods of espionage and attack; and perhaps even prevent and respond. Every categorization is subject to dispute. Some may quibble with categories here and argue we should include more or fewer. Almost every category can be called fraud; both supply chain infiltration and cyber intrusion involve computers; and IP loss at the hands of company insiders results from dozens of separate behaviors. The nine categories that follow are not so few as to lump in behaviors that differ fundamentally, and not so many as to overwhelm.

THE NINE TECHNIQUES CHINA USES TO STEAL IP

1. Consent

Consent is not theft, but the dividing line between consent and coercion can be blurry, and what often starts as consent can become coercion, reverse engineering, and outright theft. As the Wall Street Journal quoted one PRC policy maker, "China's offer to the world has been straightforward. Foreign companies are allowed to access China's markets but they would need to contribute something in return: their technology." In these cases, a foreign company agrees to give a Chinese state-owned or private enterprise IP in exchange for access to China's consumer or labor market. PRC entities may require that a certain percentage of the product be manufactured in China using a local contractor. PRC authorities also often insist that certain industries must form joint ventures with Chinese partners. General Motors, for example, created a joint technical center with Shanghai Automotive Industry Corporation (SAIC) in 1998 to transfer engineering information. In 2005 Siemens agreed to work with its Chinese partner company to build 60 high-speed trains, based on Siemens' Velaro model. A press release dated November 2005 noted that, "Part of the contractual terms and conditions involves technology transfer in connection with [the] production of the trains."

2. Coercion

In 2018, one in five members of the American Chamber of Commerce of Shanghai reported pressure to transfer technology to their Chinese partners. That pressure can take many forms. At times the PRC side can withhold information or change the terms of foreign companies' access. In this way, consent can easily morph into

coercion. Chinese business partners also conspire with the authorities to launch bogus investigations into the foreign company's operation and then the authorities insist on access to documents, files, and even passwords—which collectively grant access to IP. This happened to Micron in 2018. Central or local authorities may also launch a regulatory review, and part of the review involves requiring access to sufficient detail as to permit local competitors to duplicate the product. The chemical manufacturer, Huntsman Corporation suffered this fate in 2007.

3. Fraud

This is a broad category that encompasses misrepresentation of many kinds. A producer misrepresents itself as a licensee or customer, when in reality it is intending all along to acquire the seller's technology for its own uses and without licensing or even purchasing the foreign company's product. In 2018-2019, Huawei sought to license an export controlled, high technology glass developed by the U.S. company, Akhan Semiconductor. Akhan agreed to let Huawei examine the product for purchase on the condition that Huawei do the examination in the United States, and not attempt to reverse engineer or damage the glass. Huawei agreed but then damaged and returned only part of the product. A subsequent FBI sting revealed that Huawei had shipped part of the glass to China in an attempt to reverse engineer the product. In another example, U.S. citizen Kiet Ahn Mai posed as a legitimate customer for monolithic microwave integrated circuits (MMICs). He used his U.S. based company, MicroEx Engineering, as the supposed buyer. However, Mai subsequently sent his purchase and proprietary information to Chengdu GaStone Technology Company, an MMIC manufacturer in China owned by Yi-Chi Shih. Mai pleaded guilty to one count of smuggling. Yi-Chi Shih was convicted of multiple charges at trial.

4. Predatory Finance

Predatory finance involves sharing that often starts as consensual. Companies reveal elements of their IP to investors because the investors are soon to be owners. In so-called free look scams, investors examine the IP during due diligence but never invest. Access to investee IP depends on the type and amount of investment and control, and how much, how early, and how easily the prospective target company shares its technology. This is not to say that American, British, and Japanese investors never use such techniques domestically, but PRC companies differ in that they do so systematically, and with the assistance and protection of the PRC government. PRC authorities usually deny this last assertion, but not always, as when the Shanghai government noted in 2016 that the purpose of the Shanghai Lingang Overseas Innovation Center in San Francisco was to "…serve as a broker in technology transfer." In one example, also involving insider espionage, an investor in the company Femtometrix stole the company's tech and formed a rival company in China. In another, Shanghai Space Satellite Technology (SSST) came in as a minority investor on a joint venture (JV) with KLEO of Liechtenstein, but then sought full control of the JV in order to acquire KLEO's rights to orbital slots and telecommunication spectrum. The KLEO case involved not just predatory investment, but also lawfare.

5. Lawfare

Malign actors abuse democratic countries' legal systems to effect or protect a theft of IP, although lawfare encompasses a much broader range of goals. In the KLEO example, SSST and the other PRC-based investors filed dozens of lawsuits and even criminal complaints in Germany, Luxembourg, Liechtenstein, and the United

States against KLEO, its founders personally, and even the Liechtenstein regulatory agency and regulator. All of these efforts were designed to overwhelm KLEO, induce capitulation, and allow the PRC side to take the telecommunication and orbital rights back to China. Lawfare is a particularly effective tactic when one side has a significant advantage in resources over the other. Lawfare works so often for the PRC and its companies because they work together to mass the financial, investigatory, and protective resources of a large, powerful, sovereign state against a single foreign company, which can never match China's resources. Even when foreign companies prevail in court outside China, they cannot enforce judgments or injunctions in China. Therefore, they must overcome the additional hurdle of connecting the offending PRC malign actor to funds held abroad. Perhaps no other company has spent so much and money defending its IP from PRC legal predation as Micron, the American semiconductor producer has faced attacks via multiple mechanisms, and yet continues to do business in China.

6. Insiders: Espionage and Unintentional Sharing

IP thieves can target company insiders both as intentional, witting sources of information—spies—and also, more commonly unintentional sources. Many companies lose IP to employees and contractors. Examples abound, as this method includes the most subcategories. The PRC directs several different approaches involving insiders. One line of effort involves the more than two dozen so-called "Talent Programs," which recruit scientists and researchers from across the globe to work for Chinese companies and institutions. Many, but not all of the recruits are ethnic Chinese. The FBI describes the Chinese Talent programs as a vehicle for economic espionage. Not all talent plans involve espionage, but companies should take steps to know which of their employees are talent plan members.

The PRC government and private sector also use the 2017 Intelligence Law as a hook for inducing or coercing Chinese citizens, or even non-Chinese citizens with relatives in China into stealing IP. The 2017 Intelligence law and other similar laws and regulations are more dangerous than most American businesses realize, if they are aware of them at all. The reason is that any Chinese company, whether private or state-owned, can ask the Ministry of State Security (MSS) to acquire a particular technology, which is part of the MSS's mandate. Industrial and state sponsored espionage are one and the same; each part of the Party-State-Business triangle works together to obtain IP.

Unintentional insider leaks of IP are far more common. Employees, from the highest executives to interns give away company secrets without realizing the ramifications of seemingly simple actions. They leave passwords taped under keyboards; forget to lock their computer screens; leave documents on their desks or on public transportation; speak too loudly about work in public; post IP on social media without realizing it; they patent information that should stay secret; say too much to recruiters or potential employers (both real and fraudulent) during job interviews; help unidentified callers and email correspondents with technical problems; share information with colleagues (both real and fraudulent) who have no need to know; and on and on. PRC intelligence collectors, whether private sector or from the government, know and systematically exploit these lapses, often by misrepresenting themselves as colleagues, job recruiters, contractors, or even potential romantic partners. These collectors often work through intermediaries who establish contact with targets over the phone, via email, in person, or on social media. The methods vary, but all depend on taking advantage of employees who are distracted, trusting, untrained, careless, or some combination of all four.

7. Supply Chain Infiltration

A technically sophisticated method of IP appropriation involves seeding data collection through hardware and software that American companies procure. This method, much like cyber intrusions (discussed below) involves the electronic exfiltration of data, but the supply chain attack differs in that it depends on a purchase by the victim firm. Most of the offending products come from information and communications' technology (ICT): telephones, routers, network interface cards, switches, software (particularly firmware), Wi-Fi adapters and USB hubs. PRC companies manufacture nearly all the low-cost upstream components in ICT products. Because the manufacture of ICT items such as power supplies and integrated connector modules is not automated, it is difficult to diversify production out of China. The danger is that the ICT products that U.S. companies buy, often unwittingly from the PRC, are sending U.S. company IP to the PRC. Perhaps the best-known example of this is the Huawei back door, in which U.S. officials claimed to have found that Huawei was using its cellular network infrastructure to collect sensitive information from around the world. Another well-known example comes from Lenovo's use of pre-installed software on its laptops, which collected users' private information, including logons and passwords.

8. Simple Theft

In 2011, Mo Hailong dug up proprietary, genetically modified corn seeds from a DuPont Pioneer test field in Iowa. Mo then tried to send the seeds to his employer, Beijing Dabeinong Technology Group Company in China. A DuPont employee happened to see Mo in the field, and reported what he saw to the FBI. Mo eventually pleaded guilty to conspiracy, and served a three-year prison

sentence. Six other Chinese citizens were indicted. Five fled to China before facing trial. Charges were dropped against Mo Yun, Mo Hailong's sister, and the wife of the CEO of the Beijing Dabeinong Technology Group Company. This attempt at theft failed, but companies should wonder how many other attempts succeeded. How, for example, would DuPont Pioneer have ever known about Mo Hailong if their employee had not happened to have been in the right place at the right time.

9. Cyber Intrusion

Finally, the method that garners the most attention from the media is cyber intrusion or hacking. In 2012, then NSA Director, General Keith Alexander called cyber theft of intellectual property "…the greatest transfer of wealth in history." The damage from the intrusions we know about (e.g., Google, Microsoft, Micron, Marriott, T-Mobile, Equifax, Boeing, Dupont, etc.) is disturbing and these companies should be commended for recognizing and reporting the attacks against them. Far more disturbing are the thousands of firms that do not know they have suffered losses, and worse yet are the ones that know and still fail to report and respond. They have a duty to their employees, customers, partners, investors, stockholders, and fellow citizens to follow up on these intrusions to protect both their company and send a warning to other U.S. companies that may face similar attacks.

CONCLUSION

China steals secrets from the private sector in the United States because it is easy and profitable. Moreover, whereas the United States Government spends billions of dollars every year to protect its secrets, the government and American business together spend almost nothing to protect private sector information. That means the risk involved in stealing trade secrets is much lower than for stealing the government kind, especially, when the thieves have the protection of a large, powerful, sovereign state that is in on the crime. This state sponsorship is part of the reason that corporate spies who do manage to get caught usually face almost no consequences. As above, six of the seven people who stole DuPont Pioneer's proprietary seeds faced no punishment at all. They fled to China. The result is a system of incentives in which predatory practices yield more rewards for China–the Party, the government, and private companies – than otherwise acting as responsible players in the global market focused on original R&D. If U.S. business leaders want to protect their IP, which is estimated to represent 90 percent of S&P companies' total value, they must learn to protect themselves. China will not stop, and the U.S. government's ability to help is limited.

Glenn Chafetz has more than 30 years experience in government, academia and the private sector. He spent most of his career at CIA. He is currently Director of 2430 Group.

The author thanks Connor Giersch for his research assistance.

SOURCES

Sullivan, Laura and Cat Schuknecht. 2019. “As China Hacked, U.S. Businesses Turned A Blind Eye.” NPR: All Things Considered, April 12, 2019.
https://www.npr.org/2019/04/12/711779130/as-china-hacked-u-s-businesses-turned-a-blindeye

Chafetz, Glenn. 2023. “Defending Against State-Sponsored Espionage Targeting the U.S. Private Sector is a Team Effort,” The Cipher Brief, June 30, 2023.
https://www.thecipherbrief.com/column/alternative-perspectives/defending-against-statesponsored-espionage-targeting-the-u-s-private-sector-is-a-team-effort

Gallagher, Kelly Sim. 2023. “Foreign Technology in China’s Automobile Industry: Implications for Energy, Economic Development, and Environment,” Wilson Center: China Environment Series, Issue 6, p. 12 of pdf. Accessed August 22, 2023
https://www.wilsoncenter.org/sites/default/files/media/documents/publication/CES%206%20Feature%20Article%2C%20pp.%201-18.pdf

Peters, Gary. 2017. “The Importance of China’s Sigh-Speed Tech Transfer Policy,” Railway Technology, March 1, 2017.
https://www.railway-technology.com/features/featuretheimportance-of-chinas-high-speed-tech-transfer-policy-5748075/

Wei, Lingling, and Bob Davis. 2018. “How Beijing Systematically Pries Technology from U.S. Companies,” Wall Street Journal, September 26, 2018.
https://www.wsj.com/articles/howchina-systematically-pries-technology-from-u-s-companies-1537972066

Shatzker, Erik. 2019. “Huawei Sting Offers Rare Glimpse of U.S. Targeting Chinese Giant,” Bloomberg, February 4, 2019.
https://www.bloomberg.com/news/features/2019-02-04/huawei-sting-offers-rare-glimpse-of-u-s-targeting-chinese-giant#xj4y7vzkg

Hatch, Daniel. 2019, “Man Convicted of Exporting Semiconductor Chips to China,” Learn Export Compliance, July 30, 2019. https://www.learnexportcompliance.com/man-convicted-ofexporting-semiconductor-chips-to-china/

Harris, Dan. 2022. “Chinese Free Look Schemes to Steal Your IP,” China Law Blog, March 7, 2022.
https://harrisbricken.com/chinalawblog/chinese-free-look-schemes-to-steal-your-ip/

Bhattacharjee, Yudhijit. 2023.“The Daring Ruse That Exposed China’s Campaign to Steal American Secrets,” The New York Times, March 7, 2023.
https://www.nytimes.com/2023/03/07/magazine/china-spying-intellectual-property.html

Gui Qing, Goh, and Salvador Rodriguez. 2018. “In Silicon Valley, Chinese ‘Accelerators’ Aim to Bring Startups Home,” Reuters, May 17, 2018. https://www.reuters.com/article/cbusiness-ususa-trade-china-startups-idCAKCN1II0UG-OCABS

Goldenziel, Jill I. 2021. “Law as a Battlefield: The U.S.: China, and the Global Escalation of Lawfare,” Cornell Law Review, September 2021. https://live-cornell-lawreview.pantheonsite.io/wp-content/uploads/2021/09/Goldenziel-final11234.pdf

Chafetz, Glenn and Xavier Ortiz. 2023. “China, Lawfare, and the Contest for Control of Low Earth Orbit,” "The Diplomat,” August 10, 2023. https://thediplomat.com/2023/08/chinalawfare-and-the-contest-for-control-of-low-earth-orbit/

Lu, Shen, and Asa Fitch. 2023. “China Opens Cybersecurity Probe of Micron Amid Competition,” Wall Street Journal, March 31, 2023. https://www.wsj.com/articles/china-opens-cybersecurityprobe-of-micron-amid-competition-with-u-s-over-technology-57698d0a?mod=Searchresults_pos19&page=1

Hannas, William C., James Mulvenon, and Anna B. Puglisi. 2013. Chinese Industrial Espionage: Technology Acquisition and Military Modernization. London: Routledge, 2013. https://doi.org/10.4324/9780203630174

FBI. 2023. “What We Investigate: The China Threat: Chinese Talent Plans Encourage Trade Secret Theft, Economic Espionage,” FBI. Accessed 22 August 2023. https://www.fbi.gov/investigate/counterintelligence/the-china-threat/chinese-talentplans#:~:text=Talent%20plan%20participants%20have%20pleaded,and%20theft%20of%20trade%20secrets

Girard, Bonnie. 2019. “The Real Danger of China’s National Intelligence Law,” The Diplomat, February 23, 2019. https://thediplomat.com/2019/02/the-real-danger-of-chinas-nationalintelligence-law/

Corera, Gordon. 2023. “Chinese Spy Targeted Thousands Over LinkedIn,” BBC, August 23, 2023. https://www.bbc.co.uk/search?q=linkedin&d=HOMEPAGE_GNL&seqId=765a0260-43c6-11ee-810f-7367d7bb3bcc

Gurinavicite, Juta. 2023. “If You Haven’t Experienced a LinkedIn Scam Yet, Get Ready for One,” Forbes, June 16, 2023. https://www.forbes.com/sites/forbestechcouncil/2023/06/16/if-youhavent-experienced-a-linkedin-scam-yet-get-ready-for-one/?sh=7cf0d2cd10fc

Meyer, Bernard. 2022. “Walmart-Exclusive Router and Others Sold on Amazon & eBay Contain Hidden Backdoors to Control Devices,” Cybernews, November 3, 2022. https://cybernews.com/security/walmart-exclusive-routers-others-made-in-china-containbackdoors-to-control-devices/

U.S. Department of Commerce and U.S. Department of Homeland Security. 2022. "Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry," Department of Commerce/Department of Homeland Security, February 24, 2022. https://www.bis.doc.gov/index.php/documents/technology-evaluation/2939-22-1175-attachment-1-of-1-ict-supply-chain-assessment-report-v3-dhs-doc-signed-02-24-22/file

Barnes, Julian E. 2020. "White House Official Says Huawei Has Secret Back Door to Extract Data," New York Times, February 21, 2020. https://www.nytimes.com/2020/02/11/us/politics/white-house-huawei-back-door.html

Federal Trade Commission. 2017. "Lenovo Settles FTC Charges it Harmed Consumers With Preinstalled Software on its Laptops that Compromised Online Security," Federal Trade Commission, September 5, 2017. https://www.ftc.gov/news-events/news/pressreleases/2017/09/lenovo-settles-ftc-charges-it-harmed-consumers-preinstalled-software-itslaptops-compromised-online

Rodgers, Grant. 2016. "Chinese Businessman Gets Deal in Seed Theft Case." Des Moines Register, January 27, 2016. https://www.desmoinesregister.com/story/news/crime-andcourts/2016/01/27/chinese-businessman-pleads-seed-theft-case/79428650/

Rogin, Josh. 2012. "NSA Chief: Cybercrime constitutes the "greatest transfer of wealth in history." Foreign Policy, July 9, 2012. https://foreignpolicy.com/2012/07/09/nsa-chiefcybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/

Sullivan, Laura and Cat Schuknecht. 2019. "As China Hacked, U.S. Businesses Turned A Blind Eye." NPR: All Things Considered, April 12, 2019. https://www.npr.org/2019/04/12/711779130/as-china-hacked-u-s-businesses-turned-a-blindeye

Berman, Bruce. 2021. "Latest Data Show that Intangible Assets Comprise 90% of the Value of S&P 500 Companies," IP CloseUp, January 19, 2021. https://ipcloseup.com/2021/01/19/latestdata-show-that-intangible-assets-comprise-90-of-the-value-of-the-sp-500-companies/