CHAPTER EIGHT

Technology and Research

Technology transfers between nations exist on a spectrum of legitimacy. In many developing economies, multinational corporations willingly agree to skills and technology transfer arrangements in exchange for the right to operate. Governments support these measures in the hopes of furthering economic development. Transfers cross the threshold into illegitimacy when coercion, misappropriation, theft, or espionage are deployed with the effect of undermining a company's, and ultimately its home country's, economic competitiveness. China's expropriation of American technology is an example of how it leverages its influence among universities, corporations, and diaspora communities to further strategic objectives. This chapter reviews the targets of China's expropriation efforts, describes the state and nontraditional collectors involved, and concludes with recommendations for how the United States can better defend against this phenomenon. It is important to note that not all expropriation of intellectual property occurs at the explicit direction of the government and that China is not the sole country targeting the United States. Nonetheless, China—whether at the level of the state or individual—is considered the most serious offender.

While Chinese cyberthreats and clandestine spying against the United States dominate the public discourse, a far more serious threat is posed by China's informal or "extralegal" transfers of US technology and intellectual property (IP) theft.[1] Operating under the radar, these quiet diversions of US technical know-how are carried out by groups and

individuals in the United States, whose support for China erodes America's technological edge and ability to compete in international markets. These groups are managed by a professional cadre of Chinese government and government-associated science and technology transfer specialists who facilitate intellectual property "exchanges" through a maze of venues. They target specific advanced technologies drawn from China's industrial planning priorities (e.g., Made in China 2025[2]) such as semiconductors, robotics, next-generation information technologies (e.g., big data, smart grid, Internet of things), aviation, artificial intelligence, and electric vehicles. As a result of their efforts, a commission convened by the National Bureau of Asian Research concluded that IP theft, primarily from China, costs the American economy hundreds of billions of dollars each year, with significant impact on employment and innovation.[3] Former commander of United States Cyber Command and director of the National Security Agency General Keith Alexander was even more grave when he asserted the ongoing theft of IP by China represents "the greatest transfer of wealth in human history."[4]

The Dynamics of Chinese IP Theft

Chinese nontraditional collection and IP theft is not done randomly by individuals acting on their own. Rather, China has enacted some two dozen laws that have created a state-run foreign technology transfer apparatus that sponsors, for example, labs in China that rely wholly on information provided by compatriots working abroad. The apparatus also maintains databases of foreign co-optees and distributes stipends, sinecures, and cash to foreign donors of high-tech innovations. In addition, the apparatus is responsible for the care and feeding of agents willing to "serve China while in place" abroad.

Targets

China targets all sources of American innovation, including universities, corporations, and government labs, exploiting both their openness and

naïveté. The methods and tradecraft are custom tailored to each target. For universities, China takes advantage of the commitment to intellectual freedom on campus, which strongly resists government scrutiny of the activities of foreign students in hard-science programs and international academic cooperation. For corporations, the lure of the Chinese market gives Beijing tremendous leverage in exacting tech transfer from American firms, combined with financial incentives for employees to purloin intellectual property for personal gain. Finally, US government labs have a historical commitment to international scientific cooperation, and an uneven record of monitoring that cooperation for unsanctioned transfers of information.

These efforts complement China's legitimate efforts to invest in its own indigenous innovative capacity. China has for several decades made science and technology development a priority and appears to have the political will to see it through. This is demonstrated by the research and development (R&D) funding programs it has put into place, the investment in core scientific infrastructure that is in some cases unparalleled anywhere else in the world, and a national scientifically oriented industrial policy. Yet the continuing intense engagement in IP theft is, in many ways, an indication of the gaps in China's indigenous innovation efforts.

Once acquired, foreign technology is converted in China into products and weapons at 180 "Pioneering Parks for Overseas Chinese Scholars," 160 "Innovation Service Centers," 276 "National Technology Model Transfer Organizations," and an unknown number of "technology business incubators." These facilities are strategically located to ensure wide distribution of the foreign technologies.

Nontraditional Collectors

Nontraditional collectors include Chinese citizens, Chinese Americans whom the Chinese government is better able to cultivate or coerce, and other Americans. They range from students to researchers. Many are willing participants, such as students from Chinese defense universities explicitly tasked with acquiring foreign technology; others are not and

are targeted for access to research they have pursued by their own passion and intellect. Indeed, some nontraditional collectors may even be unwitting in their support.

Collectors do not appear to be chosen by Beijing for their race or nationality; rather they are targeted for their access to the desired intellectual property and their willingness to violate their employee agreements or national laws. Indeed, more recent scholarship has shattered the shibboleth that the Chinese government only recruits ethnic Chinese. While Chinese intelligence does have a historically strong track record of attempting to recruit ethnic Chinese, primarily because of cultural and language affinity, more recent cases of espionage and technology transfer suggest that the Chinese government has broadened its tradecraft to recruit nonethnic Chinese assets and collectors as well, perhaps as a way of complicating US counterintelligence efforts.

China's most systematic channel for identifying foreign-based nontraditional collectors is its Recruitment Program of Global Experts (海外Õ'层次人才引进计划), commonly known as the Thousand Talents Plan (千人计划) or the Thousand Talents Program (TTP).[5] The TTP is a massive and sustained talent recruitment campaign designed to recruit leading experts from overseas to assist in the country's modernization drive.

Initiated in 2008, the TTP aims to recruit leading overseas scientists and experts who work in areas that are deemed high priority for achieving China's modernization goals.[6] The program originally aimed to recruit one thousand "overseas talents" (海外人才) over a period of five to ten years. Official Chinese TTP websites list more than three hundred US government researchers and more than six hundred US corporate personnel who have accepted TTP money.[7] In many cases, these individuals do not disclose receiving the TTP money to their employer, which for US government employees is illegal and for corporate personnel likely represents a conflict of interest that violates their employee agreement.

State Collection Apparatus

China's nontraditional collection relies on a web of activities, including open-source research, exchanges, cooperation and professional organizations, direct funding of research, strategic acquisition, and cyberespionage.

Open-Source Research

China's efforts to exploit foreign innovation is further seen in its open-source acquisition infrastructure, which surpasses that of any other country. China employs a cadre of thousands to locate, study, and disseminate foreign journals, patents, proceedings, dissertations, and technical standards without regard to ownership or copyright restrictions. The documents are indexed, archived, and supplied to Chinese commercial and military "customers."

Exchanges

The Chinese government organizes and pays for exchanges in which participants travel from the United States, divulge technical knowledge through scripted venues, are briefed on China's technology interests, return to their US base to collect more information, and repeat the process. China has a program for what it euphemistically calls "short-term visits" by co-opted foreigners, which, stripped of its rhetoric, is indistinguishable from state-run espionage.

Cooperation Organizations and Advocacy Groups

Many Sino-US science and technology (S&T) "cooperation" organizations in the United States facilitate these transfers and have individual memberships of hundreds to thousands. The figure scales to some ninety such groups worldwide. Members usually are expatriate Chinese, although China is expanding its recruitment of non–ethnic Chinese. One significant example of a Sino-US S&T cooperation organization is Triway Enterprise Inc. (三立国际有限公司), an "external training institute" set up under the auspices of the State Administration of Foreign Experts Affairs in Falls Church, Virginia, with branches in Beijing and Nanjing.

According to the Chinese version of the website, the company "since 1993 has been putting its energy into promoting bilateral exchange and cooperation between China and the US in the fields of S&T, culture, education and management with great success."[8]

China S&T advocacy groups in the United States declare loyalty to China and acknowledge a "duty" to support China's development. Members visit China to lecture, guide Chinese technical projects, transfer technologies, receive shopping lists from Chinese entities, and engage in other kinds of "technical exchanges." Many of them sit on Chinese government boards that decide the future of China's national technology investment. Another example of a China S&T advocacy group is the Silicon Valley Chinese Engineers Association (硅谷中国工程师协会), which describes itself as "a non-profit professional organization formed mainly by the professionals in the Bay Area from mainland China with a mission to promote professionalism and entrepreneurship among members," which is achieved by "organizing a variety of professional activities and *establishing channels to allow members to engage in China's rapid economic development*" [emphasis added].[9]

Chinese government tech-transfer offices, facilitation companies, and career-transfer personnel, some of whom are posted to China's diplomatic offices, support and direct the US-based groups. In China, hundreds of government offices are devoted entirely to facilitating foreign transfers of technology "by diverse means."

Joint Research

The preferred method of establishing a research beachhead in the United States is through the formation of a joint research center with a prominent US university. One example is the China-US Joint Research Center for Ecosystem and Environmental Change at the University of Tennessee, Knoxville.[10] Launched in 2006, researchers from the University of Tennessee and the Department of Energy–funded Oak Ridge National Laboratory partnered with the Chinese Academy of Sciences to address "the combined effects of climate change and human activities on regional and global ecosystems and explore technologies for restora-

tion of degraded environments." The center's research focuses on science at the heart of the "green technology" revolution, which is one of Beijing's major national industrial policy objectives.

The center's website lays out three goals that match nicely with a tech-transfer agenda: (1) organize and implement international scientific and engineering research; (2) serve as a center for scientific information exchange; and (3) provide international education and technical training.[11] The website goes on to outline cooperative mechanisms to achieve these goals, including joint research projects, academic exchange, student education, and "*technical transfer and training*"[12] [emphasis added]. This dynamic differs fundamentally from the mission of Western research facilities abroad, which is to adapt technology already in their portfolios to sell in foreign markets. A PRC study on the benefits of overseas "research" to obtain foreign technology put it this way: "How can you get the tiger cub if you don't go into the tiger's den?" (不入虎穴, 焉'終凡≠).[13]

Cyberespionage

Perhaps the most damaging channel for stealing US intellectual property is cyberespionage. As noted above, NSA director Keith Alexander has called cyberespionage by Chinese state actors the "greatest transfer of wealth in human history." Cyberespionage is both a means for pilfering US science and technology and a method of intelligence collection for potential attacks against American military, government, and commercial technical systems. As a result, these cyber intrusions represent a fundamental threat to American economic competitiveness and national security.

Other Means of Misappropriation

While not technology transfer per se, counterfeiting is so common in China that it has the same practical effect. Schemes range from the subtle to blatant: benchmarking against ISO standards;[14] patent research where a design is modified slightly, if at all, re-patented in China, and "legally" produced with government protection;[15] reverse engineering;[16]

"imitative innovation" (模仿创新),[17] with or without the innovation (also called "imitative remanufacturing" 模仿改造);[18] and marketing the pirated product without or with its original logo.[19] Other reporting has detailed how the Chinese government exploits regulatory panels (often with members who have direct conflicts of interest by working for local competitors) and antitrust investigations to acquire trade secrets from foreign companies, aiding domestic industries.[20]

Conclusion and Recommendations

China's aggressive policy is threatening the advantages the United States has long enjoyed as a scientifically creative nation. This is occurring as a declining number of US students are getting advanced degrees in science and technology, R&D funds are dropping off, and the nation's manufacturing base is shrinking.[21] When combined with a more scientifically competent China that is also using the discoveries of others, the future of US competitiveness comes into question.

The best source of resiliency in the face of rampant IP theft from China is continued and expanded reinvestment in American innovation. The United States can recover its competitiveness by manufacturing what it invents and rebuilding the scientific foundation on which its competitive edge depends. But unless active efforts are made to prevent countries from inappropriately exploiting American technologies developed at great cost, efforts at national reconstruction will be wasted. The United States' current defense of intellectual property has not been effective in refuting appropriation by China, by all accounts the world's worst offender.

A key source of American creativity—the country's individualism and openness—makes it difficult to implement collective efforts to protect the products of American innovation. Nonetheless, policies and processes can be improved to reduce the risk of misappropriation without compromising the United States' innovative capacity. These require improved transparency with better information and screening, enhanced export controls, and stronger investment reviews.

Transparency, Better Information, and Screening

One of the most glaring factors that facilitates IP theft is the fact that recipients of Chinese funding programs, such as the Thousand Talents Program described above, routinely do not declare their work in China. At a minimum, recipients should be required to register as foreign agents under the Foreign Agents Registration Act (FARA).[22] Recipients who are active government employees may be breaking the law, as 18 US Code § 209 prohibits accepting supplemental income for performing the same role that falls under the scope of their government employment.[23]

The US government and universities should also make an evidence- and risk-based assessment when determining whether to admit students into major research programs. The current system, known as the Student and Exchange Visitor Information System (SEVIS),[24] is designed "to track and monitor schools and programs, students, exchange visitors and their dependents while approved to participate in the US education system." SEVIS collects data on surnames and first names, addresses, date and country of birth, dependents' information, nationality/citizenship, funding, school, program name, date of study commencement, education degree level, and authorization for on-campus employment. As of March 2011, China had the largest number of students in SEVIS, at 158,698.[25]

The FBI has access to all of the student data contained in SEVIS and no longer needs the permission of the Department of Homeland Security to initiate investigations of foreign students.[26] However, the laws, regulations, and directives governing SEVIS do not require some additional critical pieces of information, which are perceived by the Government Accounting Office (GAO) to be important to managing the program:

- The nonimmigrant visa number, expiration date, and issuing post are optional and only captured if entered into the system by the school or exchange visitor program.
- The nonimmigrant driver's license number and issuing state were imposed by the interagency working group and support investigative efforts.

- The nonimmigrant passport number, passport expiration date, and passport issuing country are optional and only captured if entered into the system by the school or exchange visitor program.[27]

It is difficult to ascertain from open sources whether these problems have been fixed, but the nonmandatory data are key investigative details that would be critical for federal law enforcement seeking to assess possible illicit technology transfers by students.

Improved Export Controls

The second major policy problem involves PRC student access to controlled technology under the deemed export system. According to the Commerce Department, a restricted product or technology is "deemed," or considered exported, when it is used by a foreign national in the United States.[28] However, under these rules, a university or research lab does not need a deemed export license if a foreign graduate student is merely present in a lab. It only needs a license if it intends to export that technology to the foreign national's country.

From 2004 to 2006, the US Commerce Department attempted to change these rules[29] but was stymied by opposition from universities and research labs.[30] Yet the continued flow of controlled technology to the PRC and the findings of GAO studies on the problems of university oversight[31] strongly suggest that Commerce's recommendations should be reexamined.

In 2009, then president Obama "directed a broad-based interagency reform of the US export control system with the goal of strengthening national security and the competitiveness of key US manufacturing and technology sectors by focusing on current threats and adapting to the changing economic and technological landscape."[32] Specifically, the initiative aimed to "build higher fences" around a core set of items, the misuse of which can pose a national security threat to the United States.[33]

The reform initiative is synchronizing the two existing control lists, the Munitions List and the Commerce Control List, so that (1) they are "tiered" to distinguish the types of items that should be subject to stricter or more permissive levels of control for different destinations, end uses,

and end users; (2) they create a "bright line" between the two current control lists to clarify which controls any given item, and reduce government and industry uncertainty about whether particular items are subject to the control of the State Department or the Commerce Department; and (3) they are structurally aligned so that they potentially can be combined into a single list of controlled items.[34]

Moreover, the lists will be transformed into a "positive list" that describes controlled items using objective criteria (e.g., technical parameters such as horsepower or microns) rather than broad, open-ended, subjective, generic, or design-intent-based criteria.[35] After applying these criteria, the list will be divided into three tiers based on their military importance and availability.[36]

On the one hand, these reforms could greatly improve the efficiency of the export control bureaucracy, preventing fewer technologies from slipping between the cracks and finding their way to China. They could also make the system and its control lists better able to keep pace with technological change, which had been a major problem with the old system, particularly with regard to fast-moving information technologies. On the other hand, the reforms appear to loosen controls over dual-use technologies, which China has a long and successful track record of integrating into advanced systems, and which can form the core of new innovations. The future of these reforms is unclear as the Trump administration appears to focus on more aggressive trade strategies and policies designed to protect US industries and punish offending Chinese companies.

Strong Investment Reviews

The Committee on Foreign Investment in the United States (CFIUS) is an interagency committee that serves the president in overseeing the national security implications of foreign investment in the economy.[37] As China's economy and financial weight has grown, CFIUS has reviewed an increasing number of proposed acquisitions of American companies and infrastructure by Chinese entities. Many of these proposed mergers have received high levels of media and congressional attention, and most of the high-profile cases have ended in rejection or strong discouragement

leading to abandonment of the deal. While the CFIUS process may have prevented individual cases of sensitive or illegal technology transfer, it could also have had the unintended effect of forcing Chinese actors to steal the data through espionage because of their inability to buy them. Recent legislation, signed by President Trump, is a substantial improvement to CFIUS, closing loopholes that the Chinese had been exploiting, and broadening the scope of the CFIUS authorities in important ways. The new law extends CFIUS review timeframes, increases the types of transactions subject to CFIUS' jurisdiction, makes certain notifications mandatory, and establishes a process for potentially expedited review and approval of certain transactions. The four new "covered transactions" include real estate deals near US national security facilities, deals involving "critical infrastructure" or "critical technologies," changes in ownership rights by a foreign investor, and any transaction designed to evade the CFIUS process. In exchange for all these additional burdens, the new law also helps companies by clarifying time limits for decisions and places important jurisdictional limits on the expansion of the law's scope.