SYM-AM-22-078

Excerpt from the Proceedings of the Nineteenth Annual Acquisition Research Symposium

Acquisition Research: Creating Synergy for Informed Change

May 11–12, 2022

Published: May 2, 2022

Prepared for the Naval Postgraduate School, Monterey, CA 93943.

Acquisition Research Program
Department of Defense Management
Naval Postgraduate School

The research presented in this report was supported by the Acquisition Research Program at the Naval Postgraduate School.

To request defense acquisition research, to become a research sponsor, or to print additional copies of reports, please contact any of the staff listed on the Acquisition Research Program website (www.acquisitionresearch.net).

Acquisition Research Program
Department of Defense Management
Naval Postgraduate School

Defensive Industrial Policy: Cybersecurity Interventions to Reduce Intellectual Property Theft

Chad Dacus—is a professor of cyber warfare studies with the Air Force Cyber College. He also serves as the Director, Air University Cyber Research Task Force. His research interests include economics and its contribution to national security and the protection of intellectual property. His writing has been published in journals such as IEEE Security & Privacy, Defense Acquisition Research Journal, and Strategic Studies Quarterly. He holds a PhD in economics from Rice University and an MS in statistics from Texas A&M University. [chad.dacus@au.af.edu]

Carl (Cj) Horn—is a professor of cyber warfare studies with the Air Force Cyber College. Previously, Cj served as the Director of the School of Joint Strategic Studies within the College of Information and Cyberspace at Fort McNair. In that position he led the nation's only War College program centered on information and cyberspace warfare. He served more than 24 years in the U.S. Army as an armor officer and strategist. Cj earned a BS in history from the U.S. Military Academy at West Point and his MA and PhD in history from The Ohio State University. [carl.horn.4@au.af.edu]

Abstract

Through cyber-enabled industrial espionage, China has appropriated what Keith Alexander, the former Director of the National Security Agency, dubbed "the largest transfer of wealth in history." Although China disavows intellectual property (IP) theft by its citizens and has set self-sustained research and development as an important goal, it is unrealistic to believe IP theft will slow down meaningfully without changing China's decision calculus. China and the United States have twice agreed, in principle, to respect one another's IP rights. However, these agreements have lacked any real enforcement mechanism, so the United States must do more to ensure its IP is better protected from China's sophisticated hackers. We call for selective interventions in nascent industries—especially those with important implications for national defense. U.S. policymakers must consider both the supply and demand aspects of the "market" for intellectual property theft to make informed decisions as to how to steer resources. This paper offers insight that the supply side of the equation has been given relatively short shrift. We offer a spectrum of potential interventions to address underinvestment in cybersecurity leading to IP theft and discuss where to go from here.

China's miraculous growth over the past 50 years has lifted hundreds of millions out of poverty. However, some of this growth has taken place at the expense of U.S. corporations who have fallen victim to intellectual property theft on an unprecedented level (Jamali & O'Connor, 2020). Until 2018, the U.S. response has primarily consisted of threats to impose sanctions and indictments of Chinese nationals who are not subject to U.S. jurisdiction. Even in 2018, when the United States imposed tariffs on Chinese goods, the Trump administration's rationale was based on unfair trade practices related to the forced transfer of U.S. technology and intellectual property rather than in retaliation for IP theft (U.S. Trade Representative, 2018). Although an economic and trade agreement signed in 2020 promises some progress on the issue, it should not be presumed that IP theft will slow down significantly (U.S.-China, 2020). Recent reports of increased criminal arrests for IP theft within China certainly provide some room for hope (The National Law Review, 2021). However, a recent policy change prevents the singling out of China because the initiative was being used as a catch-all for cases involving China and led to accusations of bias toward Asian Americans and Chinese citizens (Leslie & Liu, 2022). Given that the United States must continue under the assumption that IP theft will continue, the question becomes whether additional initiatives are necessary to help stem the flow of ideas out of the country.

This paper proposes that more be done to support U.S. organizations' cybersecurity efforts. That is, the focus of U.S. policy should turn to the supply side of the IP theft equation.

Toward that end, we begin with a brief description of the damage to the U.S. economy caused by Chinese IP theft and then proceed to outline both the economic phenomena that can cause private organizations to underinvest in cybersecurity and the benefits the Chinese accrue from pilfering IP. In this way, we lay the groundwork for the cost-benefit framework that follows. This conceptual relationship between the costs of stealing IP versus the benefits of having access to it serves as the initial inspiration for investigating the "supply side" (or U.S. innovation side) as the primary direction for policy change. This thought process is then reinforced by numerous, largely unsuccessful attempts by U.S. policymakers to address China's behavior through demand-side interventions. Finally, we present a spectrum of potential policy innovations designed to address the issue by strengthening the cybersecurity of domestic innovators. Throughout the paper, we alternate our focus between examination of domestic and Chinese phenomena and motivations, and this approach will ultimately lead to the conclusion that more strenuous efforts should be undertaken on the domestic front.

Cost to the U.S. Economy

Estimating the cost of China's cyber-enabled industrial espionage to the U.S. economy is a difficult exercise for a myriad of reasons—not the least of which is lack of specific data. For this analysis, estimates of order of magnitude will suffice. In 2019, the U.S. Patent and Trademark Office estimated that economic activity in IP-intensive industries contributed 41% of gross domestic product. In addition, the same report stated that about 44% of U.S. jobs in 2019 were in industries either directly or indirectly supported by IP-intensive industries and that these jobs paid an average of 60% higher salaries than those in non-IP intensive industries (Toole et al., 2021). The 2013 IP Commission estimated the annual cost to the U.S. economy to be comparable to the current volume (at that time) of exports to Asia, $300 billion (The Commission on the Theft, 2013). Meanwhile, the 2017 IP Commission Report cites a lower bound of $225 billion and an upper bound of $540 billion (The Commission on the Theft, 2017). Converting these figures to 2022 dollars, the inflation-adjusted bounds are $259–$621 billion. To provide an idea of scale, the revenue of the entire U.S. software market is estimated to be $314 billion in 2022 (Statista, 2022). Numerous experts, including Paul Goldstein, have sensibly cast doubt on the accuracy of these estimates, but even using a more conservative estimate backs General Alexander's assessment of an unprecedented transfer of wealth (Goldstein, 2018).

The economy-wide impact of IP theft should not completely overshadow the effects on nascent individual industries. To take one example, Chinese IP theft relating to solar panels was primarily responsible for the bankruptcy of nearly 30 U.S. manufacturing firms. To add insult to injury, many of these firms received government support through subsidies and tax incentives intended for nascent firms involved in the development and provision of energy that is less harmful to the environment ("Made in China," 2019). Another study found that the U.S.-China trade war resulting, in part, from rampant IP theft has likely contributed to a 25.7% increase in bankruptcies in the U.S. farm industry (Wu & Turvey, 2020). According to a study by the Ponemon Institute, nearly 85% of the value of the Standard and Poor's 500 is represented by intangible assets (which include both IP rights and reputation; Ponemon Institute, 2020). In particular, small businesses cannot withstand losses of this magnitude even if the losses are not sustained as cash outlays—attracting investors becomes an impossible task. The Bureau of Labor Statistics has reported that close to 50% of businesses fail within five years, so the margin of error is quite small (U.S. Bureau of Labor Statistics, 2022). Regardless of the reliability of loss estimates, the industries involved and the sheer volume of activity in innovation-intensive industries in the United States should illustrate the importance of addressing this problem more effectively.

Developing Supply and Demand for IP Theft

Supply Side: Underinvestment in Cybersecurity for Information Goods

Not only is malicious cyber activity ubiquitous, but multiple phenomena lead the private sector to underinvest in cybersecurity, thus aggravating the situation. Analysts often cite the frequent presence of externalities in the market for cybersecurity as a theoretical rationale for underinvestment. The negative externality, in this case, is the incurring of losses by those who were not responsible for securing the information technology assets that were compromised by the malicious actor(s). To take just one example, this can happen when a computer is infected and becomes a part of a botnet that victimizes thousands or perhaps even millions of other computers. In addition to externalities, several other related and unrelated theoretical explanations exist for underinvestment in cybersecurity, particularly concerning information goods, as Hal Varian and others have referred to them (Varian et al., 2004; Nabipay, 2018).

Information goods often involve low marginal costs, technological lock-in, network bundling of applications, and network effects. Each of these phenomena can foster market power. First, marginal costs are almost negligible for information goods such as software applications of various types. Another download or search engine query does not cost much to provide. Rising marginal costs have served as a competition-based limit on firm size for generations now, but this competition-enhancing mechanism is often unavailable for information goods. Next, technological lock-in occurs because users are often reluctant to switch platforms once they have adapted to new technology. A famous example of technological lock-in is the baffling long-term dominance of the QWERTY typewriter or keyboard despite its inefficiency. In the modern information age, computer operating systems are arguably the most vivid example. Switching would cost large organizations a staggering sum, and the pain would certainly be felt at the individual level. Once a vendor has you as a customer, the firm is more likely than not to keep you as a loyal customer.

When they apply, network effects can serve as a powerful force for establishing and reinforcing market power. Network effects occur when an application's value depends crucially on the number of other people who use it. Meta (formerly Facebook) is a compelling example of this phenomenon because the entire point of social media is to share ideas and experiences with others. A sparsely populated platform seems almost useless for this purpose. Of course, the more people who use a platform, the more market power that application enjoys. Finally, bundling can help kick-start network effects. For example, Microsoft arguably drove Netscape out of business by bundling its Internet Explorer web browser with its popular operating system. Netscape sued and secured a settlement but lost the war and was acquired by America Online (AOL) in November 1998. AOL stopped supporting Netscape in 2008. As one can see, powerful forces tend to influence markets for information goods to substantial market power or even monopoly. This has important implications for investment in cybersecurity.

With the above conditions often favoring the first (or among the first) application to market, firms face intense pressure to develop the application quickly. Since secure coding coursework is seldom required in computer science programs, these skills are not resident in most application developers' toolboxes without slowing their coding significantly (Lam et al., 2022). Cybersecurity suffers because a secure product that comes to market too late is not likely to garner much market share due to existing network effects and technological lock-in, so the obvious motivation is to rush it to market and get it secured later. In addition, consumers do not have tools with which to meaningfully assess cybersecurity, though Consumer Reports' Digital Lab is a step in the right direction (Consumer Reports, 2022). Concerns about underinvestment in cybersecurity are especially pronounced for smaller, less capitalized firms, with an estimated 43% of cyberattacks directed toward them (Steinberg, 2019). As mentioned earlier, these same firms may not survive a data breach that calls the exclusivity of their

intellectual property into question. Now that we have discussed the phenomena that lead to less-than-optimal cybersecurity for potential U.S. victims of IP theft, let us now examine the benefits that accrue to the Chinese when they are successful in stealing secrets.

Demand Side: Benefits of IP Theft to China and Structural Impediments to Reform Within China

Part 2 of China's latest five-year plan focuses on innovation-driven development (Center for Security and Emerging Technology, 2020). IP theft can help jump-start these efforts. The question becomes whether China is well-positioned to take advantage of the acquisition of new knowledge.[1] Several observations (not necessarily a comprehensive list) point to the Chinese faring quite well as consumers of IP theft: (1) a highly educated workforce with particular strength in product development, (2) research and development (R&D) expenditures among the world leaders and unsurpassed expenditure during the experimental development phase of R&D, (3) a socialist economy that can facilitate the transfer of the purloined secrets to those who can use it most efficiently, (4) a Chinese monetary policy that has not, until arguably recently, been focused on a strong renminbi, and (5) China's extensive experience in technology transfer and IP theft.

Among nations not defined as high-income economies, China's workforce has no peer. China stands at an impressive 12th place in the Global Innovation Index, which measures factors as wide-ranging as human capital and research, business sophistication, and infrastructure (Dutta et al., 2021). According to the Center for Security and Emerging Technology (Zwetsloot et al., 2021), China produced 46% more PhD engineering graduates than the United States in 2019 and is expected to nearly double the U.S.'s number of graduates by 2025. Although there is certainly doubt as to the relative quality of doctoral graduates in the two countries, this level of production of scholars and advanced practitioners is impressive. On this measure, China is unambiguously well-positioned to take full advantage of innovations conceived in the United States.

Although all economic data from China should be treated with a fair degree of skepticism, the Organisation for Economic Cooperation and Development (OECD) reports that China spends more on R&D than any other country except for the United States. While the United States leads the world in basic and applied research expenditure, China tops world expenditure on the last stage of R&D, experimental development. Furthermore, China's experimental development spending comprises more than a staggering 82% of its overall R&D investment (Organisation for Economic Cooperation and Development, 2021). From these data, China is arguably the best-positioned country in the world to take advantage of innovations produced elsewhere.

Deng Xiaoping popularized the phrase "socialism with Chinese characteristics" (Moak & Lee, 2015). While the Chinese approach incorporates elements of market economics, its core economic system follows the general tenets of socialism. China's five-year plans are modeled after the Soviet economic model and provide a much more detailed blueprint for economic planning than anything produced by governments in countries with market-based economies. Indeed, China has the world's largest number of state-owned enterprises (Wang, 2021). One can safely assume since the Chinese government supports these enterprises, it can set R&D priorities within the enterprises it owns to maximize the application of any purloined IP. Furthermore, it is difficult to imagine that any Chinese enterprise could resist significant

[1] A disclaimer on this discussion is that IP thieves lack the understanding involved in making the discovery themselves. The difficulties posed by this lack of knowledge are complex and beyond the scope of this research effort.

pressure from its authoritarian central government. We conclude that China's government can steer stolen IP to those it deems best positioned to use it efficiently.

China pegs the value of the renminbi to the U.S. dollar. By definition, countries peg their currencies to an anchor currency to stabilize the exchange rate and minimize exchange rate risk. However, China's motivation to do this is far weaker than it is for smaller economies with less stable economies because it has one of the largest economies in the world and a well-established currency. China has always denied manipulating its currency to keep it artificially low against the U.S. dollar. However, it is undeniable that China's economy has been buoyed by its world-leading level of exports, and a weak renminbi serves to lower the price of its exports. China's most visible actions in setting the exchange rate have served to drop the value of its currency to its lowest point in years (Feng, 2019). At a minimum, China's pegged exchange rate provides it with the opportunity to put its products in the best competitive position possible for garnering market share.

Technology transfer has long been identified as a potential accelerant of economic growth for developing countries (Gurbiel, 2002). Chinese companies are armed with a variety of methods to facilitate the transfer of advanced technologies, including foreign direct investment and joint ventures with foreign companies, venture capital investments, licensing agreements, and talent acquisition. The Chinese government often directs the acquisition to take place and actively assists (O'Connor, 2019). To provide a rough idea of scale, the Chinese participated in 10–16% of all venture deals from 2015 to 2017 (Brown & Singh, 2018). With a population of more than 1.4 billion, the lure of China's large market often proves irresistible to U.S. firms, leading to forced technology transfer. With more than 35 years of executing technology transfer, the assessment that the Chinese have mastered the art of taking technologies and adapting them for their production and use is most likely a gross understatement (U.S. Congress, Office of Technology Assessment, 1987).

China's world-leading number of PhD engineering graduates with unsurpassed experimental development R&D funds to back them is uniquely positioned to take advantage of America's basic and applied research. These well-funded and capable engineers work for organizations that are commonly experienced with technology transfer. In addition, China's powerful central government can steer any IP gains to those who can use it most efficiently and use monetary policy to enhance the cost competitiveness of its products. China denies that it condones IP theft, but this is not the case, based on American indictments of Chinese hackers and the reports of a long-standing commission to address it. China's plausible deniability is further eroded by its unwillingness to cooperate with the prosecution of IP violators. It is difficult to believe that China will slow its IP theft considerably until it becomes more difficult to acquire or there is little left of value that the Chinese do not already possess.

Cost-Benefit Visualization for Intellectual Property Theft

IP theft involves the theft of unique innovations, so an analysis based on a common static analysis of supply and demand is immediately problematic. However, this does not prevent investigating the supply and demand sides of the market in terms of cost-benefit analysis from the point-of-view of the potential thief. Benefit represents the value of the IP to the adversary that is attempting to exfiltrate it. Exactly how this might be measured is an interesting question. Projected future cash flows resulting from the acquisition are the most straightforward and intuitively reasonable metric to use, but uncertainty is likely to be pronounced. If the central government is using the hacker(s) as an agent in a particular case, the hacker may be the one estimating the perceived value to their government employer in a particular instance. Government officials' objectives could focus on cash flows but could also consider the prestige involved with acquiring the breakthrough. Regardless, estimated future cash flows generated

from the innovation will serve as a useful proxy even if it is not the exact metric used for measuring benefit. Uncertainty is assumed to be significant. Meanwhile, cost represents the difficulty involved in acquiring the IP. The effectiveness of the cybersecurity measures the firm has in place can serve as a very useful proxy for cost. Cost is measured at the "portfolio" level, as the hacker(s) may acquire information about one or more innovations while traversing the firm's network(s). Uncertainty will also be significant here but is likely to be smaller than the uncertainty involved with estimating benefit. As more information is gained through reconnaissance, this uncertainty may decrease markedly.

Figure 1 depicts a notional relationship between estimated cost and benefit for individual or firm-wide IP theft from China's point of view. The points represent either individual advances or portfolios of innovations depending on what can be exfiltrated essentially simultaneously (i.e., from a particular firm). For ease of exposition, the scales of the two axes are assumed to be identical. If the estimated benefit of the new technology is greater than or equal to the estimated cost to acquire it, then the clear choice is to attempt to eventually exfiltrate the data. For those observations near the break-even line, the calculus gets a bit murkier because of the high degree of uncertainty involved for both estimates. Since the uncertainty of benefit may well be larger than the uncertainty as to the cost, potential hackers are likely to refrain from attempting to acquire the information when the cost and benefits are nearly equal. Of course, a philosophical point is raised by all of this: What if the Chinese are attempting to hack essentially every U.S. company of any renown with multiple hackers? This supposition assumes that the Chinese have an essentially limitless number of hackers, which seems unlikely but cannot be dismissed out of hand. We will grant that it is likely that many large corporations are likely to be active targets of Chinese hackers, but it is far from clear that China's hacking labor pool is inexhaustible. Therefore, we assume the Chinese face this dilemma especially for opting to hack specific small businesses, and that the additional costs are meaningful to China's leadership and an actual choice is made based on a cost-benefit calculus.

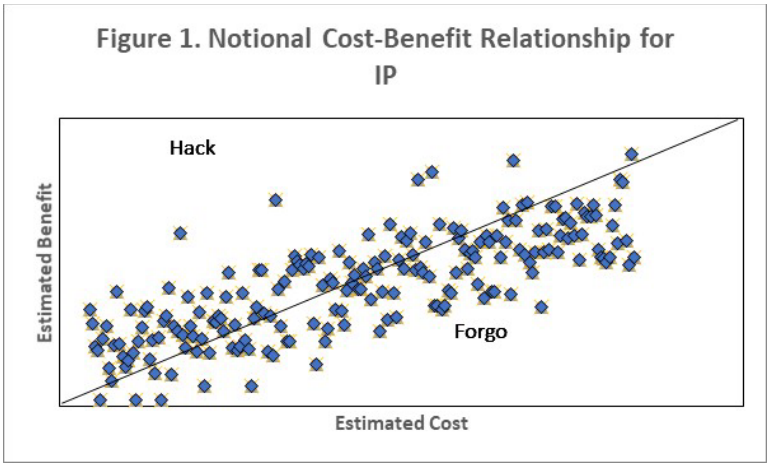

Figure 1. Notional Cost-Benefit Relationship for IP

The goal of policy is to move innovations from the "Hack" area to the "Forgo" area of the chart. To accomplish this movement, either the benefit must go down or costs must increase. Another immediate question is whether we prefer certain innovations to others when considering additional protections through policy. Now that we have a conceptual model for the decision of whether to attempt to exfiltrate trade secrets, we now turn our attention to policy interventions, and we will discover the majority of U.S. policy interventions to specifically combat IP theft have been designed to address Chinese behavior rather than to increase the cost by making the IP more difficult to pilfer.

U.S. Policy Interventions to Address Intellectual Property Theft

We begin by investigating China's history of weak IP protection and attempts by the United States to change this mindset. The basis for the conclusion of Chinese cultural indifference to intellectual property rights goes back over 2,500 years ago to Confucianism (Alford, 1997). Since Confucian philosophy is inherently collectivist, it is perhaps unsurprising that individual property rights would not be emphasized within China. Moreover, Marron and Steel (2000) identify collectivist values and developing-country status as inversely related to respect for intellectual property rights as reflected in software piracy. The United States itself has a checkered history of protecting intellectual property while it was a developing country (Peng et al., 2017).

In more recent years, the United States has harshly criticized China for its lack of protection of IP rights. This is not a particularly new source of contention between the countries—as far back as 1991 and repeatedly in the 1990s, the United States threatened to impose sanctions on China under Section 301 of the Trade Act of 1974 (Zeng, 2010). With the maturation of the Internet, Chinese IP theft remained a contentious issue, leading to a 2015 agreement between the nations not to "conduct or knowingly support cyber-enabled theft of intellectual property" (White House, Office of the Press Secretary, 2015). After some initial progress, Chinese IP theft continued at its previous pace. The United States has repeatedly indicted individual Chinese hackers for stealing intellectual property (Department of Justice, 2021). In addition, during the Trump administration, the United States levied $200 billion in tariffs on Chinese imports (U.S. Trade Representative, 2018). In 2020, the two countries entered into a Phase One agreement to protect IP, and the United States has already stated that the Chinese are failing to live up to its commitments (Lawder, 2021). In summary, the United States has been assertive in addressing Chinese IP theft from the demand side, with repeated legal, economic, and diplomatic efforts to protect U.S. innovation from the prying eyes of the Chinese. We now turn our attention to the supply side of the equation. What has the United States done to raise the cost involved in stealing IP?

U.S. efforts to specifically protect IP focus primarily on legal remedies and recoveries. The United States has strong legal protections against IP theft against prospective thieves within its borders. The United States is ranked as the leading worldwide protector of IP according to the U.S. Chamber of Commerce's Global Innovation Policy Center (2022). However, IP rights do not extend beyond the borders of the country and rely on effective IP protection laws in the country where it is used. Despite recent efforts to improve IP protection within China, there are strong structural impediments to progress (Rechtshaffen, 2020). Beyond legal remedies, the U.S. government could provide cybersecurity assistance to raise the cost to hackers to exfiltrate IP data.

The U.S. government supports numerous general initiatives to improve the cybersecurity of U.S. firms but little that is specific to IP protection. While examining (or even listing) every cybersecurity initiative of the U.S. government is far beyond the scope of this research effort, some of the more notable activities for our purposes are the design and implementation of cybersecurity standards,[2] cybersecurity threat actor information-sharing programs, free cyber hygiene services, and technical guidance resources provided primarily by the private sector (Department of Homeland Security [DHS], 2022). For critical infrastructure such as the defense industrial base, the Department of Homeland Security (DHS) and sector risk management agencies are primarily charged with ensuring the continuous availability and provision of critical

[2] Note that the primary standards, promulgated by the National Institute of Standards and Technologies, was designed for use by critical infrastructure owners and not necessarily for the consumption of all of private enterprise.

resources and functions through Presidential Policy Directive-21 (PPD-21). Although improved cybersecurity, in general, will certainly also help protect IP, PPD-21 focuses effort exclusively on the security and resilience of critical infrastructure (White House, Office of the Press Secretary, 2013). The authors were unable to find specific cybersecurity initiatives for IP beyond what is offered for general consumption. Notably, the Small Business Administration recently announced a small grant program for bolstering the cybersecurity infrastructure of emerging small businesses (U.S. Small Business Administration, 2022).

The Government Accountability Office's (GAO) recent report—DoD Critical Technologies: Plans for Communicating, Assessing, and Overseeing Protection Efforts Should be Completed—merits discussion on specific protection of IP. The DoD has broken its processes for identifying and protecting critical acquisition programs and technologies into four steps, including identifying, communicating, protecting, and assessing and overseeing the security of critical of technologies. This initiative appears to be a worthwhile extension of the DoD's current role as Sector Risk Management Agency for the defense industrial base. Steps such as including contract language for enhancement of protection efforts can certainly raise the level of protection afforded to these critical technologies (GAO, 2021). The DoD's Protecting Critical Technology Task Force has selected four promising lines of effort including "protecting the research and development enterprise, which includes academia, labs, and universities," but how much progress has been made is unclear (Lopez, 2019). The White House published the first National Strategy for Critical and Emerging Technologies (2020) and has provided an updated list of critical and emerging technologies. The Critical and Emerging Technology Update report states that a strategy on U.S. technological competitiveness and national security is forthcoming. Presumably, this follow-on strategy will contain more definitive prioritization and funding information than this report omits (National Science and Technology Council, 2022). Although these efforts are promising, gaps are likely to remain that can hopefully be partially addressed with the initiatives identified in this paper.

The United States has frequently intervened to influence Chinese behavior regarding IP theft. In addition, U.S. government organizations stand ready to facilitate the legal efforts of aggrieved parties in international courts. However, efforts to strengthen the cybersecurity of innovators specifically to protect IP are lacking. Since the overall effectiveness of U.S. efforts to stem the flow of secrets out of the country has been universally regarded as relatively unsuccessful, we turn our attention to what might be done to improve the situation through cybersecurity assistance.

Protecting Our Most Valuable IP: Defensive Industrial Policy

Since attempting to stem Chinese IP theft through influencing Chinese decision-making seems to have largely failed to this point, the United States should move to shore up defenses. This will involve the shifting of resources to selective nascent industries for defensive purposes. We describe this action as defensive industrial policy, which is distinct from the established concept of industrial policy. Industrial policy is defined as "government intervention in a specific sector which is designed to boost the growth prospects of that sector and to promote the development of the wider economy" (Dadush, 2016). For defensive industrial policy, rather than attempting to boost growth prospects, the purpose is to protect the growth prospects of a nascent sector and the resulting development of the entire economy. The obvious question is how to choose which innovations to protect. We return to our supply and demand framework to answer this question.

To get a good sense of innovation occurring within the United States, one can start with the federal agency responsible for granting patents, the U.S. Patent and Trademark Office (USPTO). Although the patent, copyright, and application for patents and copyrights data this

office maintains will represent far from a full picture of U.S. innovation, the inventor's financial interest acts as a powerful incentive to apply for a patent for new technology that can or will be marketable in the near future. However, software developers may not choose to file a patent because the process is too lengthy, costs an average of $50,000, and may not be reliably enforceable against infringement (Chang Villacreses, 2020). In addition, there is no single data field within the patent and copyright data to quickly identify that a particular innovation involves a particular technology, such as artificial technology. Perhaps ironically, Giczy et al. (2022) found the need to use a sophisticated machine learning approach for a recent analysis of artificial intelligence patents. Considering these disclaimers, patents, copyrights, and applications for each could be useful as an initial input into what technologies the United States should prioritize.

For innovations that may have national security implications, the USPTO performs an initial screening and, if national security concerns are evident, refers the application to the appropriate agency. For prioritizing innovations important to national security, this data could be invaluable. In addition, this data set is likely to be much less cumbersome than the full data sets maintained by the USPTO. Of course, this process is unlikely to be free of error, and some inventions may eventually become important or be revealed as important to national security, but this should serve as a basis from which to begin the analysis. As mentioned earlier, the National Science and Technology Council (2022) has generated a list of critical and emerging technologies that could also prove to be invaluable.

Another avenue for identifying important technologies is to use the words and actions of the Chinese. China's five-year plans (FYP) sketch the social and economic development initiatives planned by the Chinese Communist Party and can be a helpful, if perhaps somewhat lagging, indicator of China's R&D priorities. The question becomes whether these plans are predictive of what industries Chinese hackers choose to target. To establish the veracity of this link, we can compare industries identified in China's 12th FYP to Department of Justice indictments from 2014 to 2018 (the alleged thefts took place between 2011 and 2015). We choose to use indictments rather than other sources, such as news articles containing accusations, so that clear attribution rests on a relatively solid foundation. Table 1 lists the industries identified in the FYP with companies named as targets (if specified).

Table 1. 2011–2015 U.S. Industries Allegedly Targeted by Chinese Hackers
(Central Committee of the Communist Party of China, 2011, DoJ, 2014; DoJ, 2017; DoJ, 2018).

Industry Identified in FYP	Year(s) Indictment Occurred	Company(ies)
Energy conservation	2014	SolarWorld
New generation IT	2018	Multiple (unspecified), MSS Cloudhopper
Biological	2018	Unspecified
High-end equipment	2017, 2018	Boeing, Trimble (GPS), Unspecified
New energy	2014	SolarWorld
New material	2014, 2018	Westinghouse, Unnamed
Petrochemical	2018	Unspecified
Light	2014	Unspecified
Textiles	2014	DuPont*
Maritime	2018	Huntington Ingalls
Iron and steel	2014	U.S. Steel
Non-ferrous metals	2014	Alcoa
Building materials	2014	DuPont

These results confirm broad agreement between China's stated policy targets and the illicit activity of Chinese hackers for these years. This data is admittedly dated, and it remains to be seen whether this agreement between policy and hacking behavior will continue. Nevertheless, using the FYPs appears to be a fruitful way to identify IP that may require additional protections. Of course, this should not be the only source of information on China's targets for IP theft. Intelligence reports and investigations of industry claims of Chinese IP theft could also prove quite helpful. If national security concerns are to be prioritized, the industries and technologies identified as ripe targets could be evaluated for their potential importance to national security. Now that we have identified some ways to select industry segments to protect, we turn our attention to what kind of interventions might be helpful.

Spectrum of Interventions to Protect IP

Since the United States has pursued the Chinese on IP theft to a relatively strenuous degree and with underwhelming results, the U.S. government should actively consider policies to strengthen the protection of valuable IP on a technical level. The level of analysis and data required to arrive at the preferred portfolio of policies is beyond the scope of this paper, but we will sketch a general outline of the spectrum of interventions that may prove beneficial. The status quo will represent the lower end of the spectrum with far more active interventions occupying the opposite extreme. Information-sharing efforts and the new DoD process for protecting critical technologies described by the GAO (2021) should be included as a matter of course.

As discussed earlier in the paper, the United States is already actively involved in public-private initiatives to shore up cybersecurity, particularly regarding critical infrastructure. While there is not much in the way of assistance for IP protection, in particular, the critical infrastructure initiatives involve industries likely to have produced and to continue producing the innovations that will protect future national security and fuel economic prosperity. For example, PPD-21 names the Defense Industrial Base Sector as a critical infrastructure sector with the DoD serving as its Sector Risk Management Agency (White House, Office of the Press Secretary, 2013). Under PPD-21, the Secretary of Homeland Security

> evaluates national capabilities, opportunities and challenges in protecting critical infrastructure; analyzes threats to, vulnerabilities of, and potential consequences from all hazards on critical infrastructure; identifies security; identifies security and resilience functions that are necessary for effective public-private engagement with all critical infrastructure sectors; develops a national plan and metrics, in coordination with SSAs and other critical infrastructure partners; integrates and coordinates Federal cross-sector security and resilience activities; identifies and analyzes key interdependencies among critical infrastructure sectors; and reports on the effectiveness of national efforts to strengthen the Nation's security and resilience posture for critical infrastructure. (White House, Office of the Press Secretary, 2013)

This is certainly an impressive list of support activities, but (1) protection of IP is not mentioned as a priority, rather the focus is squarely on resilience (though these security efforts would help with the protection of IP too), (2) the list of duties is so numerous as to be arguably overwhelming and makes it questionable whether the DHS and the Sector Risk Management agencies can truly accomplish all of the duties to more than a superficial level, and (3) the list of identified critical infrastructure sectors is quite lengthy itself, again placing enormous demands on the DHS and sector risk management agencies. Risks that involve the stealing of IP but do not threaten the functionality of critical infrastructure are likely to be discounted due simply to a

lack of available personnel and/or funds to address the concern. Aside from critical infrastructure protection, the federal government supports numerous other initiatives that have spillover benefits to the protection of IP, but all of them pale in comparison to its efforts to protect critical infrastructure.

Beyond the status quo, the federal government could provide cybersecurity grants. As mentioned earlier, the U.S. Small Business Administration (SBA) announced it will grant $3 million to strengthen the cybersecurity infrastructure of new small businesses (SBA, 2022). A similar program for smaller businesses with promising IP might help small businesses avoid theft that might put them out of business. In 2018, small businesses accounted for 43.5% of U.S. gross domestic product (Kobe & Schwinn, 2018). Meanwhile, according to The Small Business Guide to Cybersecurity (SCORE, 2020), up to 71% of cyberattacks occur at businesses under 100 employees. There is a lot of variability in these estimates from different sources and years—CPO magazine estimates that 50% of all cyberattacks (Powell, 2019). Regardless, most estimates indicate malicious cyber activity aimed at small businesses outstrips the businesses' contribution to the GDP. Alarming statistics abound when studying the behavior of our adversaries versus small businesses. According to Barracuda Networks (2022), the average employee of a small business with fewer than 100 employees fields 350% more social engineering attempts than an employee of a larger enterprise. Although it is impossible to prove, available data suggests that small businesses underinvest in cybersecurity. Juniper Research (2018) found that small businesses make up only 13% of the overall cybersecurity market. Meanwhile, small businesses make up 99% of all U.S. businesses (SBA, 2020). It seems that adding a grant program specifically for companies with promising IP to the U.S. government's existing efforts could be a step in the right direction. Although Information Sharing and Analysis Organizations (ISAO) are not government organizations, the formation of an ISAO focused on the protection of intellectual property would be beneficial. These organizations can help spread threat-specific information and best practices to innovators across the country.

The U.S. government could go beyond grants to provide some active assistance itself. For example, the U.S. government could field specialized teams to either consult with promising small businesses or provide cybersecurity services to businesses directly. At the extreme, this would be much more interventionist and require a high degree of trust between the parties. This would put these teams into direct "competition" with private-sector cybersecurity service providers but might still prove helpful to businesses that may not be informed consumers of these services.

Many of the same services provided to critical infrastructure providers could also be provided to those organizations with valuable IP. These services include a multitude of basic services provided to the public with many additional services available to critical infrastructure providers (Cybersecurity + Infrastructure Security Agency, 2021, Fall). DHS could survey these services and determine which to promulgate in a more specialized form to organizations with valuable IP.

The final question to address is how any aid might be prioritized between sectors. Reflecting on the government's approach to cybersecurity assistance writ large, critical infrastructure sectors immediately spring to mind. In addition, selecting national security as the paramount national interest for cybersecurity assistance makes sense for several reasons. First, a nation whose security is threatened will be much less able to protect any of the other national interests including ensuring the prosperity of its citizenry. Second, defense spending, in general, has been found to increase economic growth (Sheremirov & Spirovska, 2022), so spending designated to protect R&D gains with national security implications would intuitively boost economic growth to an even greater extent.

Conclusion

China has been stealing U.S. IP for decades. Through examination of both the costs and benefits of IP theft through a supply and demand approach, we have found that the United States has focused almost exclusively on attempting to reduce Chinese hacking through diplomatic and economic means rather than shoring up its own corporations' cybersecurity. We recommend augmenting the current approach to include cybersecurity initiatives aimed specifically at protecting IP. We have provided a spectrum of possible interventions spanning from the status quo to grant programs, additional training materials, and providing specialized teams to actively assist with shoring up cybersecurity for IP protection.

References

Alford, W. (1997). *To steal a book is an elegant offense: Intellectual property law in Chinese Civilization.* Stanford University Press.

Barracuda Networks. (2022). *Spear phishing: Top threats and trends.* https://assets.barracuda.com/assets/docs/dms/Spear-phishing-vol7.pdf

Brown, M., & Singh, P. (2018). *China's technology transfer strategy: How Chinese investments in emerging technology enable a strategic competitor to access the crown jewels of U.S. innovation.* Defense Innovation Unit Experimental.

Bureau of Labor Statistics. (2022, March 7). Business employment dynamics: Establishment age and survival data. Total private. Bureau of Labor Statistics. https://www.bls.gov/bdm/us_age_naics_00_table7.txt

Center for Security and Emerging Technology. (2020). *Proposal of the Central Committee of the Chinese Communist Party on drawing up the 14th five-year plan for national economic and social development and long-range objectives for 2030* (English translation). Georgetown University. https://cset.georgetown.edu/wp-content/uploads/t0237_5th_Plenum_Proposal_EN-1.pdf

Central Committee of the Chinese Communist Party. (2011, January). The 12th five-year plan for economic and social development of the People's Republic of China (English translation). British Chamber of Commerce in China.

Chang Villacreses, D. (2020, November 4). *Protecting your software ideas: to copyright or patent.* https://otc.duke.edu/news/protecting-your-software-ideas-to-copyright-or-to-patent/

Consumer Reports. (2022, February 22). Consumer Reports joins non-profit cyber coalition [Press release]. https://www.consumerreports.org/media-room/press-releases/2022/02/consumer-reports-joins-non-profit-cyber-coalition/#:~:text=New%2C%20global%20organization%20of%20nonprofits,help%20people%20protect%20their%20data&text=YONKERS%2C%20N.Y.,nonprofits%20dedica

Cybersecurity + Infrastructure Security Agency. (Fall 2021). *Services.* https://www.cisa.gov/sites/default/files/publications/FINAL_PDFEPUB_CISA%20Services%20Catalog%202.0.pdf

Dadush, U. (2016, February 1). Industrial policy: A guide for the perplexed. Carnegie Endowment for International Peace. https://carnegieendowment.org/2016/02/01/industrial-policy-guide-for-perplexed-pub-62660

Department of Homeland Security. (2022, March 30). *Shields up*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/shields-up

DoJ, Office of Public Affairs. (2014, May 19). U.S. charges five Chinese military hackers for cyber espionage against U.S. corporations and a labor organization for commercial advantage [Press release]. https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

DoJ, Office of Public Affairs. (2017, November 27). U.S. charges three Chinese hackers who work at internet security firm for hacking three corporations for commercial advantage [Press release]. https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations

DoJ, Office of Public Affairs. (2018, December 20). Two Chinese hackers associated with the Ministry of State Security charged with global computer intrusion campaigns targeting intellectual property and confidential business information [Press release]. https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

DoJ. (2021, November 19). Information about the Department of Justice's China initiative and a compilation of China-related prosecutions since 2018. https://www.justice.gov/archives/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related

Department of the Treasury. (2019, August 5). Treasury designates China as a currency manipulator [Press release]. https://home.treasury.gov/news/press-releases/sm751

Dutta, S., Lanvin, B., Leon, L. R., & Wunsch-Vincent, S. (2021). *Global innovation index 2021.* World Intellectual Property Organization. https://www.globalinnovationindex.org/userfiles/file/reportpdf/gii-full-report-2021.pdf

Feng, E. (2019, August 5). China's currency falls to lowest exchange rate in 11 years. *NPR*. https://www.npr.org/2019/08/05/748155575/chinas-currency-falls-to-lowest-exchange-rate-in-11-years

GAO. (2021). *DoD critical technologies: Plans for communicating, assessing, and overseeing protection efforts should be completed.* https://www.gao.gov/assets/gao-21-158.pdf

Giczy, A., Pairolero, N., & Toole, A. (2022). Identifying artificial intelligence (AI) innovation: A novel AI patent dataset. *The Journal of Technology Transfer, 47*, 476–505.

Goldstein, P. (2018, April 10). Intellectual property and China: Is China stealing American IP? [Interview by S. Driscoll.] https://law.stanford.edu/2018/04/10/intellectual-property-china-china-stealing-american-ip/

Gurbiel, R. (2002). *Impact of innovation and technology transfer on economic growth: The Central and Eastern Europe experience.* Warsaw School of Economics.

Jamali N., & O'Connor, T. (2020). "U.S., China's cold war is raging in cyberspace, where intellectual property is a costly front." *Newsweek*. September 16, 2020.

Juniper Research. (2018, August 8). Cybersecurity breaches to result in over 146 billion records being stolen by 2023. https://www.juniperresearch.com/press/cybersecurity-breaches-to-result-in-over-146-bn

Kobe, K., & Schwinn, R. (2018). *Small Business GDP: 1998–2014.* U.S. Small Business Administration. https://cdn.advocacy.sba.gov/wp-content/uploads/2018/12/21060437/Small-Business-GDP-1998-2014.pdf

Lam, J., Fang, E., Almansoori, M., Chatterjee, R., & Raj, A. G. (2022). Identifying gaps in the secure programming knowledge and skills of students. *SIGGSE 2022*, pp. 1–7.

Lawder, D. (2021, April 30). U.S. says China has fallen short on "Phase 1" intellectual property commitments. *Reuters*. https://www.reuters.com/business/us-says-china-has-fallen-short-phase-1-intellectual-property-commitments-2021-04-30/

Leslie, R., & Liu, B. (2022, March 4). U.S. Justice Department puts an end to controversial China Initiative. *Lawfare*. https://www.lawfareblog.com/us-justice-department-puts-end-controversial-china-initiative

Lopez, C. T. (2019, November 26). "Task Force Curbs technology theft to keep Joint Force strong." *DoD News*. https://www.defense.gov/News/News-Stories/Article/Article/2027555/task-force-curbs-technology-theft-to-keep-joint-force-strong/

Made in China 2025 and the future of American industry: Hearing before the Senate Small Business and Entrepreneurship Committee. (2019, February 29). 116th Cong., 1st Session. https://www.sbc.senate.gov/public/_cache/files/0/9/090fe492-3ed9-4a1a-b6c1-ebdecec39858/1AB7520770B9032F388CC9E94C79321B.glaser-testimony.pdf

Marron, D., & Steel, D. (2000, April). Which countries protect intellectual property? The case of software piracy. *Economic Inquiry, 38*(2), 159–174.

Moak, K., & Lee, M. (2015). *China's economic risk and its global impact.* Palgrave Macmillan.

Nabipay, P. (2018). *Essays on economics of information goods* [Doctoral dissertation, University of Minnesota]. http://conservancy.umn.edu/handle/11299/202166.

National Science and Technology Council. (2022, February). *Critical and emerging technologies list update*. Fast Track Action Subcommittee on Critical and Emerging Technologies. https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf

O'Connor, S. (2019). *How Chinese companies facilitate technology transfer from the United States.* United States-China Economic and Security Review Commission. https://www.uscc.gov/sites/default/files/Research/How%20Chinese%20Companies%20Facilitate%20Tech%20Transfer%20from%20the%20US.pdf

Organisation for Economic Cooperation and Development. (2021). *Gross domestic spending on R&D.* Organisation for Economic Cooperation and Development [Data set]. https://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm

Peng, M., Ahlstrom, D., Carraher, S., & Shi, W. (2017, March). History and the debate over intellectual property. *Management and Organization Review, 13*(1), 15–38.

Ponemon Institute. (2020). *Financial impact of intellectual property & cyber assets: 2020 Aon-Ponemon global report.* Aon-Ponemon Institute. https://www.aon.com/getmedia/6e200c08-c579-4333-b5f2-385ab6fbefde/Financial-Impact-of-Intellectual-Property-

Powell, M. (2019, June 25). 11 eye-opening cyber security statistics for 2019. *CPO Magazine*. https://www.cpomagazine.com/tech/11-eye-opening-cyber-security-statistics-for-2019/

Rechtschaffen, D. (2020, November 11). How China's legal system enables intellectual property theft. *The Diplomat*. https://thediplomat.com/2020/11/how-chinas-legal-system-enables-intellectual-property-theft/

SCORE. (2020). *The small business guide to cybersecurity.* https://www.score.org/resource/small-business-guide-cybersecurity

Sheremirov, V., & Spriovska, S. (2022). Fiscal multipliers in advanced and developing countries: Evidence from military spending. *Journal of Public Economics, 208*.

Statista. (2022). *Technology markets: Software. United States*. Statista. https://www.statista.com/outlook/tmo/software/united-states

Steinberg, S. (2019, October 13). Cyberattacks now cost companies $200,000 on average, putting many out of business. *CNBC*. https://www.consumerreports.org/media-room/press-releases/2022/02/consumer-reports-joins-non-profit-cyber-coalition/#:~:text=New%2C%20global%20organization%20of%20nonprofits,help%20people%20protect%20their%20data&text=YONKERS%2C%20N.Y.,nonprofits%20dedica

The Commission on the Theft of American Intellectual Property. (2013). *The IP Commission Report: The report of the commission on the theft of american intellectual property.* U.S. Patent and Trademark Office. https://www.nbr.org/wp-content/uploads/pdfs/publications/IP_Commission_Report_Update.pdf

The Commission on the Theft of American Intellectual Property. (2017). *Update to the IP Commission Report: The theft of american intellectual property: Reassessments of the challenge and United*

States policy. U.S. Patent and Trademark Office. https://www.nbr.org/wp-content/uploads/pdfs/publications/IP_Commission_Report_Update.pdf

The National Law Review. (2021, July 27). Criminal arrests for intellectual property crimes in China up 99% in H1 2021. *The National Law Review*. https://www.natlawreview.com/article/criminal-arrests-intellectual-property-crimes-china-99-h1-2021

Toole, A., Miler, R., & Rada, N. (2021). *Intellectual property and the U.S. Economy.* U.S. Patent and Trademark Office. https://www.uspto.gov/sites/default/files/documents/uspto-ip-us-economy-third-edition.pdf

U.S. Chamber of Commerce Global Innovation Policy Center. (2022). *2022 International IP index: Compete for tomorrow* (10th ed.). https://www.valueingenuity.com/wp-content/uploads/2022/02/GIPC_IPIndex2022_Report_Full_v2.pdf

U.S.-China. (2020, January 15). Economic and trade agreement between the government of the United States and the government of the People's Republic of China. https://ustr.gov/sites/default/files/files/agreements/phase%20one%20agreement/Economic_And_Trade_Agreement_Between_The_United_States_And_China_Text.pdf

U.S. Congress, Office of Technology Assessment. (1987). *Technology transfer to China.*U.S. Government Printing Office.

U.S. Small Business Administration. (2020). *2020 Small Business Profile.* https://cdn.advocacy.sba.gov/wp-content/uploads/2020/06/04144224/2020-Small-Business-Economic-Profile-US.pdf

U.S. Small Business Administration. (2022, January 21). SBA Administrator Guzman announces new pilot program to bolster cybersecurity infrastructure of emerging small businesses.

U.S. Trade Representative. (2018, June 15). USTR issues tariffs on Chinese products in response to unfair trade practices. https://ustr.gov/about-us/policy-offices/press-office/press-releases/2018/june/ustr-issues-tariffs-chinese-products

Varian, H., Farrell, J., & Shapiro, C. (2004). *The Economics of Information Technology: An Introduction.* Cambridge University Press.

Wang, T. (2021, June 14). Explainer: Why does China have so many state-owned enterprises? *Chinese Government Television Network (CGTN)*.

White House, Office of the Press Secretary. (2013). Presidential policy directive—Critical infrastructure security and resilience/PPD-21. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

White House, Office of the Press Secretary. (2015, September 24–25). President Xi Jinping's state visit to the United States [Fact sheet]. https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-State-visit-united-States

Wu, Y., & Turvey, C. (2020). The impact of the China-USA trade war on U.S. Chapter 12 farm bankruptcies. *Agricultural Finance Review, 81*(3), 386–414. https://doi.org/10.1108/AFR-05-2020-0076

Zeng, K. (2010). *Trade threats, trade wars: Bargaining, retaliation, & American coercive diplomacy.* University of Michigan Press.

Zwetsloot, R., Corrigan, J., Weinstein, E., Peterson, D., Gehlhaus, D., & Fedasluk, R. (2021). *China is fast outpacing U.S. STEM PhD growth: CSET data brief.* Center for Security and Emerging Technology. https://cset.georgetown.edu/wp-content/uploads/China-is-Fast-Outpacing-U.S.-STEM-PhD-Growth.pdf

Acquisition Research Program
Naval Postgraduate School
555 Dyer Road, Ingersoll Hall
Monterey, CA 93943

www.acquisitionresearch.net