Economic Espionage and Knowledge Diffusion Under US-China Rivalry*

Andrew Kao† Karthik Tadepalli‡

March 20, 2025

Abstract

We examine how US-China rivalry affects knowledge diffusion, by studying how economic espionage affects firms. Compiling a comprehensive dataset of publicly disclosed espionage incidents from 1995-2024, we first establish that espionage has sizable negative effects on firms. In an event-study design, revenues and R&D expenditures at targeted firms decline by 20-30% within three years, which persists for up to a decade. Espionage also has industry-level effects; US exports in targeted sectors decline by 60% over a decade, while Chinese exports rise by a similar amount, with a net result of 10% less global trade in these sectors. We examine how firms restrict knowledge diffusion in response to espionage. Although we find no evidence of firms reducing their knowledge sharing through patenting, we do find suggestive evidence that firms discriminate against ethnically Asian scientists after espionage. Overall, espionage reshapes technological advantage in the US and China, and could distort the allocation of scientific talent.

*We are grateful to Jesse Shapiro, David Yang, Andres Rodriguez-Clare, Ben Faber, Pete Klenow, Chad Jones, Carolyn Stein, Kirill Borusyak, Matilde Bombardini, Elhanan Helpman, Pol Antras, Fred Heiding, John Sturm Becko, audiences at the Berkeley Trade Lunch and the Harvard Political Economy Lunch, and especially Daniel Gross for invaluable feedback. We are also grateful to Jeremy Wu, Alex Nowrasteh, MIT Technology Review and the Center for Strategic and International Studies for their work in compiling cases of espionage, without which this study would not be possible. Both authors acknowledge support from the NSF Graduate Research Fellowship.

†Harvard University, Department of Economics. andrewkao@g.harvard.edu

‡University of California Berkeley, Department of Economics. karthikt@berkeley.edu

1 Introduction

Knowledge diffusion in the 21st century is defined by geopolitics. The US's current dominant knowledge base across many industries, from semiconductors to agriculture, has led to conflict with China over knowledge diffusion (Miller, 2022; Hvistendahl, 2021). On one side, China's Thousand Talents Program aims to draw Chinese scientists and engineers from the US to build up Chinese industry with their knowledge. On the other side, the US's China Initiative aggressively prosecuted potential links to China by researchers, seeking to clamp down on knowledge flows to China. Many firms are reluctant to share information abroad, fearing imitation by competitors (García-Vega and Huergo, 2011). Given the importance of knowledge spillovers for economic growth, restrictions on knowledge sharing due to geopolitics could have large welfare consequences. This makes it important to understand: how do firms change their production and sharing of knowledge because of US-China competition?

We study this question in the context of economic espionage. Economic espionage against Western firms on behalf of China is an especially geopolitically-charged form of knowledge diffusion. After all, espionage is simply knowledge transfer without permission. It represents efforts by Chinese firms or the Chinese state to obtain a knowledge base that would make them more productive. As China ramps up espionage efforts, firms could become more security-conscious and less willing to share knowledge with their peers. For example, they could be less willing to disclose their innovations, or less willing to share knowledge between employees—with negative consequences for the diffusion of knowledge and economic growth. As a result, economic espionage is an important empirical footprint in the cat-and-mouse game of geopolitical knowledge restrictions.

Despite its clear importance, espionage has historically been studied through individual case studies, due to a lack of systematic data. To solve this issue, we compile a comprehensive dataset on publicly disclosed economic espionage incidents, based on prosecutions under the Economic Espionage Act since 1996 and publicly disclosed cyber intrusions. China is the beneficiary country in 80% of cases in our data, facilitating the interpretation of this espionage as primarily impacting US-China knowledge diffusion. We link this case-level data to firms. This allows us to use an event-study framework to estimate the impact of espionage on firm outcomes. We find that espionage has large negative effects on targeted firms. Being successfully targeted for espionage reduces firm revenue and R&D spending by 20-30% after 3 years. These results are robust to

alternative identification strategies, and they hold for a variety of other firm outcomes. Importantly, we find no effect on either of these outcomes when espionage attempts are unsuccessful (i.e. no knowledge was transferred). This placebo test suggests that our estimated effects are not driven by violations of the parallel trends assumption. Thus, as the first stage of our analysis, we find that espionage has large negative effects on targeted firms.

Does espionage simply affect firms who are targeted, or does it affect US industry as a whole? We map espionage incidents to industries based on the primary sales sector of targeted firms, and subsequently link incidents to international trade flows in the affected industries. On a 10 year horizon, we find that Chinese exports in targeted sectors increase by 60%, with American exports in these industries declining by a similar amount. Global exports in targeted sectors decline by 10%, suggesting that the harms to the US are larger than the benefits to China. Thus, espionage affects not only the individual farms involved, but also has aggregate consequences for US industry and Chinese industry.

We then explore the effect of espionage on firms' knowledge sharing behavior. Do targeted firms reduce their knowledge sharing, especially with China? We study two margins of response: knowledge-sharing through patenting, and screening out employees perceived as "high espionage risk". We estimate the first margin of response by linking firms to their patents, and the second margin through matched employer-employee data from LinkedIn. Across a variety of outcomes, we do not find firms restricting knowledge-sharing through patenting: espionage does not affect the patent-R&D ratio, or the probability that a firm patents with an inventor in China, or how many times the firm's patents are cited. These surprising results suggest that firms do not see knowledge embodied in patents as an important source of espionage risk.

However, we do find suggestive evidence that espionage leads to firms to discriminate against ethnically Asian scientists (who they may perceive as "high espionage risk"). The number of Asian scientists declines by more than the number of non-Asian scientists in targeted firms (50% vs 30%, though this difference is noisy). Asian scientists who switch companies obtain more senior positions, while those who stay see their career progression slow down. In contrast, non-Asian scientists' careers are unaffected regardless of whether they leave. This discrepancy suggests differential selection pressure on Asian scientists, which could reflect discrimination, although it is imprecisely measured.

Together, our results point to both direct and indirect harms of espionage. They suggest that the future of declining knowledge diffusion between the US and China is unlikely to show up fully in patent data, and will instead come from restrictions on the hiring and promotion of scientific talent.

Related Literature This paper relates to four strands of the literature. First, we contribute to research on geopolitical tensions and knowledge diffusion. The growing literature on geopolitical tensions has primarily focused on trade and investment relationships between countries (Clayton, Maggiori, and Schreger, 2023), with knowledge/technological relationships between countries being much more difficult to study. Some papers within this framework that study knowledge diffusion focus on academic scientific relationships between the US and China (Flynn et al., 2024; Jia et al., 2022), or industrial espionage during the Cold War (Glitz and Meyersson, 2020). Our contribution is to study how US-China tensions affect knowledge diffusion between firms across countries, and knowledge production within firms rather than academia.

Within this literature, our paper is most closely connected to a recent paper by Curti et al. (2023), about how corporate innovation responds to the theft of trade secrets. Relative to this paper, we make three contributions. First, their analysis focuses only on how targeted firms change their innovation behavior; we focus on a much broader set of firm outcomes, in particular looking at how knowledge sharing changes as a result of espionage. Second, we analyze the aggregate industry-level effects of espionage, rather than focusing only on the harms to targeted firms, allowing us to characterize the benefits of espionage to China and harms to the rest of the world. Finally, our dataset of espionage incidents is more comprehensive in scope (164 incidents compared to 52 incidents), making our analysis informative despite the difficulty of observing espionage empirically.

Second, our paper relates to the literature on endogenous growth and knowledge diffusion. Knowledge diffusion has long been recognized as central to economic growth, for allowing ideas from one country to benefit economic growth in all countries (Eaton and Kortum, 1999). Similarly, knowledge diffusion is often incorporated into trade models to enhance the gains from globalization (Buera and Oberfield, 2020). However, this literature primarily takes the diffusion of knowledge as limited only by exogenous frictions. In reality, limiting the diffusion of knowledge could be an active choice by firms or governments. Our contribution to this literature is to test for the presence of

endogenous restrictions on knowledge diffusion in the context of US-China competition.

Third, we speak to the literature on creative destruction and business dynamism. The classic Schumpeterian model of firm dynamics and growth (Klette and Kortum, 2004) has been a guiding framework for understanding how firms creatively destroy one another through innovation. Building on the Schumpeterian model, recent work on US business dynamism highlights "knowledge diffusion"—the ease with which ideas spread from a leader firm to other firms in an industry—as the central factor explaining the decline in US business dynamism (Akcigit and Ates, 2023). Our setting provides an unusual empirical window into this process, because economic espionage directly represents ideas spreading from a leader firm to other firms in an industry. Thus, our findings about the effect of espionage provide useful stylized facts to be incorporated into future models of business dynamism and industry growth.

Finally, we speak to the small literature on the Economic Espionage Act and its consequences. Kim (2018) and Fang and Li (2021) analyze EEA cases through the lens of whether they are discriminatory towards ethnically Chinese defendants. Relative to this literature, we use the EEA primarily as a window into economic espionage, how it affects firms, and how it affects knowledge diffusion. However, we also contribute by suggesting a new dimension of discrimination from counter-espionage policies—that occurring within targeted firms.

The rest of this paper is organized as follows. Section 2 describes the context of economic espionage and the US-China relationship. Section 3 describes the construction of our database of espionage incidents and other data sources used, and provides descriptive statistics on our data. Section 4 examines the direct effects of espionage on targeted firms and industries. Section 5 analyzes how firms endogenously respond to espionage through employment and patenting. Section 6 concludes.

2 Context

From Roman monks stealing the secret of silk making from China in the 6th century, to George Washington and Alexander Hamilton endorsing a program to target the British textile industry to gain "secrets of extraordinary value," economic espionage has long been a tool of statecraft. For example, in the 19th century, the US chemical industry grew to the technological frontier through hiring German chemists who brought trade secrets (Hounshell, 1988). Espionage is even more salient under geopolitical compe-

tition. After World War II, the US recruited hundreds of German scientists through Operation Paperclip, recognizing their importance in the oncoming Cold War. During the height of the Cold War, East Germany kept pace with West Germany in its industrial development through espionage against West German industry (Glitz and Meyersson, 2020). In short, countries catching up to the technology frontier through economic espionage has a long history.

Today, espionage is believed to be widespread. For example, the security firm McAfee (Alperovitch et al., 2011) makes the staggering claim (emphasis not added):

> I am convinced that every company in every conceivable industry with significant size and valuable intellectual property and trade secrets has been compromised (or will be shortly), with the great majority of the victims rarely discovering the intrusion or its impact. In fact, I divide the entire set of Fortune Global 2,000 firms into two categories: those that *know they've been compromised* and those that *don't yet know.*

The Economic Espionage Act The United States' approach to economic espionage underwent a fundamental shift with the passage of the Economic Espionage Act (EEA) in 1996. Prior to the EEA, trade secret theft was primarily addressed through civil litigation, leaving prosecutors with limited tools to combat state-sponsored economic espionage. The Act established two key criminal offenses: theft of trade secrets to benefit foreign entities (Section 1831) and domestic trade secret theft (Section 1832). Penalties under Section 1831 are particularly severe, reflecting Congress's concern about foreign economic espionage, with individual defendants facing up to 15 years imprisonment and fines up to $5 million.

The EEA's focus has evolved significantly over time. Its initial motivation was based on concerns about industrial espionage by France, who had made it clear that they wanted to develop a computer industry to compete with the US's computer industry, and were suspected of using industrial espionage to aid with that process (Times, 1991). However, in the 2000s, the focus shifted toward China, reflecting broader changes in geopolitical tensions and technological competition. From 1997-2008, defendants of Chinese descent represented 17% of EEA prosecutions. This proportion increased dramatically to 52% during 2009-2015 (Kim, 2018). This shift coincided with China's rapid technological advancement, and increasingly explicit policies aimed at acquiring foreign technology and expertise.

US-China Rivalry and Espionage As China has grown, it has pursued ways to gain knowledge from the US. These efforts are exemplified by the Thousand Talents Program, launched by China in 2008. The Thousand Talents Program represents one of China's most significant efforts to acquire foreign technology and expertise. It aimed to recruit leading international scientists, researchers, and entrepreneurs to work in China, with a particular focus on those with expertise in strategic technologies and access to intellectual property at major Western institutions. By 2018, over 7,000 individuals had participated, including both Chinese nationals working abroad and foreign scientists. Although research collaboration in most forms can be legitimate, the program has also been used to facilitate unauthorized technology transfer, including several incidents in our sample. The Thousand Talents Program evolved significantly after receiving heightened scrutiny. China has stopped publicizing information about participants and rebranded various components of the program.

In the context of countering the Thousand Talents Program, the US Department of Justice launched the China Initiative in 2018. The China Initiative marked an aggressive shift in US law enforcement's approach to Chinese economic espionage. The initiative prioritized investigating and prosecuting cases involving technology theft benefiting China, with a particular focus on academic and research institutions. It represented the first time the DOJ had focused its national security resources explicitly on a single country, and made it clear that the US was going to invest in countering China's talent program.

The China Initiative expanded traditional counterintelligence work in several ways. It increased scrutiny of research collaborations, requiring academics to disclose Chinese funding sources and affiliations. For example, the FBI maintains a page about China's talent plans (FBI, 2020). This page proactively warns companies and academic researchers about the risk of espionage from their students and employees (emphasis added):

> Talent plans can sometimes foster legitimate sharing and collaboration as part of an appropriate business arrangement or research exchange, but this is not the norm. Instead, talent plans usually involve undisclosed and illegal transfers of information, technology, or intellectual property that are one-way and detrimental to U.S. institutions. *Your students and/or employees could be talent plan participants.*

The China Initiative also broadened prosecution strategies, using tools like grant

fraud charges and failures to disclose foreign ties rather than relying solely on evidence of direct technology theft. This enabled prosecutions even without direct evidence of unauthorized technology transfer.

By 2021, the DOJ had brought over 70 cases under the initiative, charging both Chinese nationals and American citizens, particularly those of Chinese descent. However, the initiative faced mounting criticism over its implementation. Civil rights organizations argued it disproportionately targeted Asian-American scientists - one study found that 88% of defendants charged with grant fraud were of Chinese heritage (Guo, Aloe, and Hao, 2021). Critics argued that the initiative's broad scope created a chilling effect on legitimate scientific collaboration and contributed to racial profiling in academia and industry science. In January 2022, the New York Times documented a high-profile dismissal of all charges against MIT professor Gang Chen (Times, 2022), bringing the criticism of the China Initiative to its peak. Just one month later, the DOJ ended the China Initiative, replacing it with a broader "Strategy for Countering Nation-State Threats", which eliminated China-specific branding, though it has maintained a focus on Chinese espionage.

Vignettes of Economic Espionage It is useful to characterize what incidents of economic espionage actually look like. An archetypal incident would be David Yen Lee, a former technical director at Valspar Corp, a company that makes paint. Lee illegally downloaded trade secrets from Valspar and Huarun (a Chinese subsidiary of Valspar) to an external thumb drive, with the intention of giving these secrets to the Shanghai office of Nippon Paint, a Japanese paint company, where he had accepted a vice-president position. However, he was arrested before he could actually deliver the information to Shanghai (FBI, 2010). This mechanism of espionage—an individual downloading information illegally with the benefit of financial reward and employment in China—is representative of many cases. This case also exemplifies an "unsuccessful" case of espionage—where no information was actually leaked from Valspar. This kind of case will later be important for assessing the credibility of our results.

Another case comes from Orbit Irrigation, a company that manufactures sprinkling and irrigation systems. Janice Kuang Capener was in charge of operations at an Orbit plant in China from 2003 to 2009. She provided proprietary information about Orbit's pricing strategy to Zhejiang Hongchen Irrigation Equipment, a Chinese competitor to Orbit, which they used to undercut Orbit's position in the market (DOJ, 2015). This

case demonstrates that economic espionage is not always about the theft of technology, but is sometimes about economic information/market research that can also be important to businesses.

Caveat Our research examines the economic impacts of espionage on firms. But we are aware of the political and racial undertones of discussions about Chinese economic espionage. Indeed, a large number of economic espionage cases do not involve a foreign country at all, but instead represent domestic corporate espionage (Fang and Li, 2021). In our dataset and analysis, we focus on foreign economic espionage and Chinese economic espionage in particular, because we believe that setting is most appropriate for understanding the effects of US-China geopolitical rivalry, and because Chinese economic espionage is an active policy issue of large importance. But as the China Initiative shows, there is a fine line between countering Chinese espionage and persecuting ethnically Chinese researchers. As Kim (2018) and Fang and Li (2021) show, Economic Espionage Act prosecutions are systematically biased against ethnically Chinese defendants. Thus, our paper should not be taken as a justification to lower the standards of evidence for alleging economic espionage.

3 Data and Descriptive Statistics

To examine the impacts of economic espionage on victim firms and their responses, we construct a novel dataset that combines information on espionage incidents with detailed firm-level outcomes. This section outlines the key data sources and the construction of our analysis sample.

3.1 Espionage Data

Our primary data on economic espionage come from court filings, Department of Justice (DoJ) announcements, and reports from relevant think tanks. This dataset compiles all publicly documented cases brought under the Economic Espionage Act since its enactment in 1996, as well as other instances of foreign economic espionage against US firms since 1990, focusing on cases targeting non-defense firms. For the purposes of this study, we define economic espionage as theft of proprietary economic information—these are most often technological trade secrets, but may also include confidential information such as business development or pricing strategies. We do not focus on

explicit technology transfer, such as through China's *quid pro quo* policy (Holmes, McGrattan, and Prescott, 2015). We also omit cases where the only data stolen is customer information, such as data breaches of emails or passwords, since this kind of information is not central to a firm's economic advantage over its competitors.

Sample construction To build a comprehensive database of incidents of economic espionage against the United States, we compile all information from the following sources:

1. All Department of Justice (DOJ) press releases about economic espionage indictments,[1] alongside relevant publications such as the DOJ's Pro IP Act Annual Reports.

2. CourtListener, a non-profit legal research database that contains legal data from a variety of sources, including the commonly used Public Access to Court Electronic Records (PACER) data. This combined with the press releases above supersets the dataset used by Fang and Li (2021) to study the Economic Espionage Act.

3. Reports and articles on espionage. These come from a wide range of actors, such as the Cato Institute (Nowrasteh, 2021), the Center for Strategic and International Studies (Rostker et al., 2023), investigative journalists (Guo, Aloe, and Hao, 2021), legal scholars (Kim, 2018) and concerned citizens (Wu, 2024).

4. Our own search of news articles, corporate press releases, and cybersecurity firm announcements.

All of these sources are necessary to develop a comprehensive picture of economic espionage, because not all incidents are pursued or prosecuted by the US government (and so may not appear on the DOJ websites or court filings). We manually confirm whether each economic espionage incident occurred or not, and collect the following information for each incident: date espionage began, date espionage ended (if distinct), earliest date espionage was reported or announced to the public, whether the suspect successfully obtained the proprietary information, the suspect's country, whether this was a cybersecurity incident or not, alongside the victim companies targeted, and the suspect firm (when available).

[1]There are roughly 50 of these websites in addition to `www.justice.gov`. We manually verify any economic espionage incidents in the roughly 3,000 webpages returned after a keyword search of 'economic espionage' across these websites.

We manually code whether an espionage incident was "successful", meaning that the attempt to steal trade secrets was successful and the information was delivered to some beneficiary, or "unsuccessful", meaning that the attempt was not successful. This distinction is generally unambiguous from the descriptions of cases in press releases or court documents.

Descriptive Statistics We uncover 164 cases of attempted economic espionage in our primary sample. Of these, 126 are successful (77%, cases where the suspect successfully delivered the proprietary information to the intended target), and 129 of these are attributed to China (79%). We show a timeline of espionage incidents in Figure 1.

In Table 1, we provide a list of industries (SIC codes) targeted more than once by espionage, as well the number of times these industries have been targeted. These industries, such as semiconductors, plastics, pharmaceuticals, and aircraft manufacturing, tend to be knowledge-heavy in nature, as well as reliant on trade secrets to protect their competitive advantage. More than three-quarters of our incidents take place in a repeatedly targeted industry. In Figure 2, we plot the rank of victim firm revenues (before espionage) relative to their industry. We find that targeted firms tend to be leaders in their industry: in over half of cases, they are one of the three largest firms in their 4-digit SIC code. However, the same pattern does not hold when examining firms relative to their 3-digit SIC code: targeted firms are spread much more evenly through the firm rank distribution in their 3-digit SIC code.[2] This implies that the targeting of firms occurs within a 4-digit SIC code rather than the 3-digit code. Thus, the 4-digit SIC code is likely to provide the best definition of a targeted industry.

Analysis of Suspects While the dataset identifies victim firms comprehensively, limited information exists on the perpetrators of espionage. Only 27 cases involve suspect companies that are publicly traded, which constrains our ability to analyze effects of espionage on perpetrator firms. We are unable to identify a suspect firm in the majority of cases for a variety of reasons: many individuals who conduct espionage incidents intend to found their own start-up or give the information to a small enterprise for which we cannot find data. In other cases, espionage is attributed to foreign universities or government agencies (such as the Chinese Ministry of State Security), making it unclear which firms precisely benefit from espionage. Thus, our analysis of

[2]See Figure A.1, Panel C. In Panel B and D, we replicate these plots using R&D expenditures and show that the same patterns hold when examining the rank of firm R&D expenditures.

the effects of espionage on China uses international trade data from UN COMTRADE, which allows us to examine the aggregate spillover effects of economic espionage across countries.

Sample Selection We acknowledge a major limitation of our study; we can only observe espionage in the selected set of cases that are detected and reported. This set may be very different from the typical espionage case, that may be undetected at all, or only detected by a security firm and never reported to the world. Thus, we cannot claim to offer a full accounting of the welfare costs of economic espionage, or an understanding of the average espionage case (which may be very different from what we observe).

All of our results should be interpreted in the context of this selected sample. However, for our research question, economic espionage incidents are better understood as a window into the future of firm openness, US-China knowledge diffusion and geopolitical rivalry. In that regard, selecting the most high-profile and important cases is an advantage, rather than a disadvantage, because these cases are more likely to drive changes in US-China knowledge diffusion than the unknown cases that may be more representative.[3]

3.2 Firm-Level Data

Out of 164 cases of economic espionage, we are able to identify a victim firm in 130 incidents.[4] There are 142 unique firms that we identify as targeted by espionage (some incidents target more than one firm). Of these 142 firms, 108 are ever publicly listed (or are subsidiaries of listed firms), allowing us to collect detailed financial information on them. Of these public firms, 75% of cases are successful incidents, and 83% are attributed to China.

Firm Financial Data To analyze the economic consequences of espionage, we draw on firm-level fundamentals from Compustat (for American firms) and Worldscope (for

[3]We further note that, insofar as there are cases that we do not observe, the total effect of economic espionage must be larger than that which we estimate.

[4]Court filings often redact specific victims of espionage, necessitating the use of contextual information to identify the victim firm—for instance, finding the company that a suspect worked for during the espionage period on LinkedIn, cross-referenced against industry and geographical information made available. However, this is not always possible, leading to a number of cases in which we cannot identify a victim firm.

international firms), standard sources for financial and operational data on publicly traded firms. This provides us with each publicly traded firm's revenue, R&D expenditures, total assets, intangible assets, gross margins, and net profit margins. We collect data on all firms targeted by espionage, as well as all firms sharing a SIC or SIC-3 code with these firms. This leads to a total of 23,830 firms in our main sample. We use data from 1995 to 2024 on a quarterly basis. We also supplement this data with Compustat's segments data to decompose a firm's sales across locations and industries.

For firm-level stock market returns, we rely on CRSP (for American firms) and Datastream (for international firms). We additionally make use of the standard Fama-French factors made available through WRDS to measure normal stock returns for all firms.

Firm Employee Data We examine how firms respond to espionage through their employment composition by using data from Revelio Labs. This dataset, derived from LinkedIn, provides granular information on a firm's workforce composition. Unlike the data sources above, every single victim firm that we identify has a LinkedIn page, allowing us to analyze outcomes for non-public firms as well. Revelio predicts the race of each employee based on their name, classifying at the level of "Asian" rather than "Chinese".[5] We primarily focus on employment of Asian versus non-Asian employees in the US.

Revelio classifies all job titles into 1500 different categories—we use these categories to identify whether an employee does scientific/R&D work in their role. We manually classify these categories based on whether they are likely to conduct research and development work (examples of scientists include "Clinical research", "Process development engineer", or "Scientist"). 8.7% of all employees in our sample are classified as scientists. Finally, from Revelio, we also collect employment counts across countries to investigate the geography of employment. This data allows us to understand how firms respond to espionage through their employment of scientists, as well as to detect racial heterogeneity that could reflect China-specific concerns.

Firm Innovation and Knowledge Flows We also link firm-level patent and innovation outcomes using data from the United States Patent and Trademark Office

[5]This is an unfortunate limitation of the data that we cannot address, because Revelio does not provide names for us to do a more fine-grained classification ourselves. We acknowledge there is some risk of attenuation from misclassifying whether an employee is Chinese or a different Asian ethnicity.

(USPTO). This database provides comprehensive information on firm-level patenting activity, including location of collaborators, and those who cite these patents. Even in our set of publicly listed firms in high-technology industries, patenting is relatively rare, with 75% of firm-years recording no patents at all. Thus, we focus our analysis of patents on the extensive margin; whether firms patent at all in a given year, and conditional on patenting, who they patent with. From patent records, we pull inventor information, to understand how firms to respond to espionage through the characteristics of inventors on their patents. In particular, we use the address of inventors to characterize where they live, to understand whether espionage leads firms to reduce patenting with inventors living in China or outside the US in general. Finally, we use patent citation information to measure whether patents by targeted firms are any less likely to cite Chinese patents, or to be cited by Chinese patents. Together, these measures give us a rich understanding of how firms endogenously change their knowledge flows with China and the rest of the world in response to espionage.

4 Direct Effects of Espionage

This section focuses on estimating the direct effect of economic espionage on firm revenues and innovation behaviors. This is a first stage of analysis before we can explore any second-order effects of espionage. For example, if espionage has no effects on firm revenues, we should not expect knowledge diffusion to change as a result of espionage. Thus, in this section we investigate the direct effects of economic espionage on targeted firms and industries.

4.1 Effects on Targeted Firms

To estimate the causal effects of economic espionage on firm outcomes, we employ a dynamic difference-in-differences framework. This approach leverages variation in the timing of espionage incidents across firms to identify treatment effects, as well as which firms are ever targeted, while accounting for firm-specific and sectoral trends. We discuss the multiple complementary approaches to estimating causal effects below.

Within-Sector Event Study Our core empirical specification for understanding how espionage affects firm revenue and R&D is given by the following dynamic two-way fixed effects (TWFE) regression:

$$y_{i,t} = \sum_{k=-8}^{20} \gamma_k D_{i,t+k} + \alpha_i + \alpha_{j(i),t} + \varepsilon_{i,t} \tag{1}$$

where i denotes a firm, t a quarter, and $j(i)$ the industry firm i belongs to. We interpret the timing of treatment to be when espionage *started* against a targeted firm. $D_{i,t-k} = 1$ if a firm i was successfully targeted for espionage at or before quarter $t+k$. The coefficients γ_k trace the evolution of outcomes before and after espionage begins, allowing us to examine both the pre-trend dynamics and post-treatment effects on various firm outcomes.

An important feature of this specification compared to a standard event study is that our quarter fixed effects are actually industry-quarter fixed effects. In other words, we are comparing targeted firms to untargeted firms *within the same industry*. This feature is important because industries are could be selected in whether they are targeted for espionage or not, based on the trends of firms in that industry. Thus, we want to control for industry-specific trajectories when determining whether espionage affects a firm.

To facilitate interpretation of our results and extend the time horizon over which we can measure effects, we interpret espionage as an absorbing treatment. That is, for any firm targeted multiple times by espionage, we use the first time it experiences an incident as the treatment date, and drop later espionage events. Standard errors are clustered at the firm level. The key identifying assumption is that in the absence of espionage, the outcomes of targeted firms would have evolved similarly to those of untargeted firms within the same industry.

We estimate effects on two main firm outcomes: revenue and R&D expenditures. We use revenue as a summary statistic for how much firms are affected by the loss of the competitive advantage they previously had from having proprietary knowledge/technology. However, the *welfare* effects of espionage are likely to be dominated by how it affects firm innovative activity. As a result, we use R&D expenditures to capture this dimension of the effects of espionage.

Figure 3, Panel A, plots the dynamic treatment effects on firm revenue and R&D expenditures for firms hit by an espionage incident. We find that both outcomes decline by 20 to 30% within 3 years of espionage beginning, with effects continuing to persist in the 2 years that follow. These results show that firms substantially shrink (or fail to grow) as a result of economic espionage, and the decline in R&D expenditures suggests

that espionage may have important consequences for a firm's innovativeness. A lack of pre-trends supports a causal interpretation of these results.

Placebo Test: Unsuccessful Cases In addition to the standard pre-trends test, our setting allows a unique approach to testing the validity of our identifying assumption. The key feature of our setting is that we not only observe successful espionage cases, we also observe cases of espionage that *failed*—i.e. no knowledge was transferred out of the targeted firm. This usually happens because the attempt to steal knowledge was detected and stopped before the theft could occur successfully. This is illustrated by the case of Valspar and David Yen Lee discussed in Section 3. There are 38 such cases in our dataset.

If we make the assumption that *successful and unsuccessful cases do not differ in ways that are correlated with differential post-espionage trends*, then the sample of unsuccessful cases actually allows us to test whether the parallel trends assumption holds in the *post*-period. Formally, let $S_i = I[\text{espionage on } i \text{ is successful}]$. Then under the assumption that

$$\mathbb{E}[y_{i,t}(0)|D_{i,t} = 1] - \mathbb{E}[y_{i,t}(0)|D_{i,t} = 0] \perp S_i \tag{2}$$

estimating equation 1 in the set of *unsuccessful* cases ($S_i = 0$) provides a direct test of the parallel trends assumption. This set of cases is excluded from our main estimation sample. If our empirical design is valid, we expect to find no significant effects in this placebo sample ($\gamma_k = 0$ for $k > 0$), as no actual knowledge theft occurred. Any significant effect detected in this placebo sample would be evidence of a violation in parallel trends. Conversely, a null effect in this placebo sample provides evidence for the parallel trends assumption—stronger support than is normally available in difference-in-difference designs.

In Figure 3 Panel B, we plot results for the placebo test using unsuccessful cases of espionage, and find null results, also supporting a causal interpretation of our main estimate. Failed attempts to steal information do not harm the targeted firms.

Mechanisms To understand the mechanism through which espionage reduces firm revenue and R&D, we conduct two heterogeneity analyses. First, we separate cases based on the damages claimed by the firm in court. Panels A.1 and A.2 of Figure 4 report this heterogeneity analysis. We find that our estimated revenue effects are more

negative for incidents that have a higher value of claimed damages.[6] These claimed damages represent the value of technology that was stolen, so this results suggests that the mechanism for espionage to hurt firms is that the stolen information has a high economic value. Indeed, for cases with below-median claimed damages, there is no effect of espionage on R&D. This mechanism is also a reassurance that our results are not driven by small-sample issues—even if we could get significant effects by chance in a small sample, it would be unlikely to generate heterogeneous effects by the claimed value of court damages.

Second, we separate cases based on concentration in the targeted firm's industry, proxied by HHI estimated in the data at the SIC 4-digit level. Panels B.1 and B.2 of Figure 4 show that the negative effects of espionage primarily manifest in low-HHI industries. Recall that targeted firms are typically leaders in their industry (Figure 2). So this results implies that firms mainly suffer from espionage when they have many followers, rather than only a few followers. This could be because when there are many firms, it is more likely that one of them produces a good that is highly substitutable with the targeted firm's product.

Together, these heterogeneity analyses show that the value of the stolen information and the concentration of the targeted firm's industry are important determinants of when espionage is harmful to firms.

Additional Analyses We briefly report additional analyses, which are described in more detail in Appendix Appendix A. First, as an alternative empirical strategy with different assumptions, we estimate the effect of espionage with a matched-pair design, comparing targeted firms with firms in adjacent industries that are similar among many characteristics. The results are similar to our main results (Figure A.2). Second, while our main specification is a dynamic two-way fixed effects estimator, we show that our results are robust to a variety of alternative event-study estimators (Figure A.3). Third, to examine the longer-run effects of espionage and address measurement error in the timing of espionage, we re-run our analysis at the year level, and find that effects of espionage persist a decade out (Figure A.4). Finally, in addition to firm revenue and R&D expenditures, we show that espionage also reduces a firm's total assets and

[6]It is worth noting that in Panel A.1 alone, we see pre-trends for the revenues of firms targeted in high-damage incidents; however, this pattern does not appear in any other heterogeneity analyses or in our main analysis. With enough sample splits, we would find pre-trends even if they do not drive the results, so we do not try to interpret this.

intangible assets by a similar amount (Figure A.5), that both domestic sales and exports decline (Figure A.6), and that these firms' cumulative abnormal returns decline after both the onset of espionage and when espionage is announced, consistent with losses from both real factors and the market's perception of these incidents (Figure A.7).

4.2 Effects on Targeted Industries

From a policy standpoint, what matters more than effects on targeted firms is the *aggregate* effect of espionage. If targeted firms lose revenue and conduct less R&D, but non-targeted firms gain revenue and conduct more R&D, the net result could be zero, simply reflecting a reallocation between firms. Policymakers would be much less concerned about espionage in that case, at least if the reallocation happened in the US. In this section, we estimate the industry-level effects of espionage, to net out some firms winning and others losing.

Effects on exports by US and China We test how espionage incidents affect exports in both the US and China. We prefer trade data to measure industry-level effects for three reasons. First, it covers all firms operating in each country, including non-publicly listed firms. Second, in Ricardian trade theory, exports reveal a country's productivity in a sector, so changes in exports can be interpreted as the best proxy for changes in industry productivity. Finally and most importantly, exports are the only way by which we are able to estimate how espionage affects China. For the rest of the analysis, we cannot reliably link incidents to suspect firms, and even if we could, the benefits of espionage could be diffused across Chinese industry. Therefore, looking at how Chinese exports evolve in targeted sectors is key to understanding the other side of the equation.

We map SIC codes to HS6 codes using the 2018 revision of the concordance from Pierce and Schott, 2012, and define treatment at the industry level as the first period in which an industry is *ever* targeted by an espionage incident. In other words, we keep only the first time any firm in the industry was targeted. In this specification, our never-treated HS6 codes are "nearby" codes—they share an HS4 code with a targeted HS6 code, but are never themselves targeted for espionage. Our baseline specification

is, for the outcome log(exports by country i in sector s at year t):

$$y_{i,s,t} = \sum_{k=-4}^{10} (\gamma_k D_{s,t+k} + \beta_k D_{s,t+k} \mathbb{I}[i \text{ is US}] + \delta_k D_{s,t+\tau} \mathbb{I}[i \text{ is CN}]) + \alpha_{i,s} + \alpha_{i,t} + \epsilon_{i,s,t} \quad (3)$$

Regressions are at the exporter-HS6-year level, and include exporter-HS6 and exporter-year fixed effects.[7] Apart from the direct treatment effect, we also conduct triple differences, interacting time to treatment with the exporter being the US or China. For interpretation of coefficients, in this section, we restrict cases to only to the 129 cases where the suspect country is China.

We plot results in Panel A of Figure 5. We find that ten years after espionage occurs, exports by China rise by 60%. In contrast, exports by the US fall by 60%, and exports from the rest of the world fall by 10%. This suggests that espionage increases Chinese industry productivity and harms US industry productivity. However, the net global effect is negative, with exports from the rest of the world also falling as a result of espionage. Thus, the benefits to China from economic espionage come at a global cost.

These effects are surprisingly large. Are they due to selection of which industries are targeted for espionage? China may be targeting espionage in sectors where it will anyways gain a comparative advantage due to other technology investments. We test this with the same placebo test as before: under Assumption 2, we can test whether these effects are due to espionage by estimating Equation 3 in the sample of unsuccessful cases. Panel B of Figure 5 reports the result of this placebo test. Here, the placebo test is not as clean as before. We see no decline in exports from the US or the rest of the world, suggesting that the effects on the US and the rest of the world from Figure 5 are truly causal. However, we do see Chinese exports rising in sectors even when espionage is unsuccessful. Thus, it's possible that our detected effects on China are overstated, although our conclusion that the US and the rest of the world suffer aggregate losses from espionage is more validated.[8]

[7] We do not include HS6-year fixed effects, so as to be able to plot the event study coefficients for the rest of the world as a comparison point to the US and China coefficients.

[8] We note two additional reasons that effects may be large. First, many targeted firms are large, multiproduct firms, and so losses in affected HS-6 codes may be larger than the average losses the firm faces. Second, on a ten year horizon, the loss in revenue for targeted firms is similar in magnitude to the decline in exports (see Figure A.4).

Effects on other firms in targeted industries What happens to other US firms when one of them is targeted for espionage? To address this question, we modify Equation 1 to a triple difference specification. Now, we are interested in the effects of espionage on US firms in the same industry (SIC 4-digit code) as targeted firms. In this analysis, our never-treated group is firms in *nearby* SIC 4-digit codes—i.e. firms in the same SIC 3-digit code $k(i)$ but not in the same SIC 4-digit code $j(i)$. Let $D_{j(i),t+k} = 1$ if firm i is in an SIC $j(i)$ that has been targeted for espionage. As in Equation 3, treatment is now defined as the first time an industry is targeted for espionage. Then the estimating equation is

$$y_{i,t} = \sum_{k=-8}^{20} \gamma_k D_{i,t+k} + \sum_{k=-8}^{20} \gamma_k D_{j(i),t+k} + \alpha_i + \alpha_t + \varepsilon_{i,t} \tag{4}$$

We plot results of estimating Equation 4 in Figure 6. Panel A.1 reveals that the competitors of victim firms experience relative gains to their revenue in the aftermath of espionage, on the order of 10%. This is consistent with Figure A.6, Panel B, where we showed that victim firms experience declines in domestic sales as well—it is possible that competitors are able to sell more to meet demand, and capture market share from victims. However, Panel A.2 shows that competitors to victim firms do not increased their R&D expenditures in response to espionage, hinting towards aggregate losses in innovative capacity. Panel B shows that there is essentially no response by competitors to unsuccessful cases of espionage.

Note that the sign of revenue effects being opposite does not indicate that the two effects offset each other, because firms differ in size. Ideally, we would aggregate revenue and R&D measures to the industry level and estimate an industry-level version of Equation 1 to directly test whether industry sales fell. Unfortunately, this aggregation is far too noisy to deliver informative results, so we can only make statements at the firm-level.

5 Knowledge Diffusion Under Espionage

The previous section has established the direct effect of espionage on firm and industry outcomes. But we are also interested in how espionage could affect knowledge diffusion in targeted firms and industries. This serves as a window into how geopolitical rivalry could affect aggregate knowledge diffusion in the future. Thus, in this section, we focus

on how knowledge diffusion evolves after espionage, through endogenous responses by targeted firms and employees at targeted firms.

5.1 Patent-Based Openness

One way to understand firm openness/knowledge-sharing with the world is through patenting behavior. Patenting inherently involves disclosure of inventions, providing knowledge spillovers to the rest of the world. In addition, patenting data includes information about how the technology was produced that are indicative of how internally open the firm is. Thus, we can get a richer understanding of how espionage affects knowledge diffusion through measuring patenting outcomes.

We estimate Equation 1 with patent-based outcome measures, with two differences. First, because we are especially interested in how firms respond to geopolitically sensitive incidents and US-China competition, we restrict our focus to the cases where China is the beneficiary of espionage. Second, we define "treatment" as when espionage against a firm *ends*, rather than when it begins.[9]

A natural concern with adapting Equation 1 is that now our treatment is an *information* shock, not a technology shock—and untargeted firms can respond to this information shock. Put differently; Airbus cannot (directly) lose revenue because Boeing was targeted for espionage, but Airbus can restrict its knowledge sharing in response to Boeing being targeted for espionage. By comparing the response of targeted and untargeted firms, we are implicitly assuming that untargeted firms cannot respond to the information shock provided by espionage. However, in Appendix Appendix A.2, we show that untargeted firms do not seem to change their knowledge-sharing in response to espionage against their competitors. Thus, this exercise can recover the effect of espionage on knowledge-sharing.

We first estimate the effect of espionage on the propensity for firms to patent. In Figure 7, Panel A, we show that firms targeted by espionage are about 20-30% less likely to patent in the 5-10 years following an espionage incident. This decline in innovation

[9]Previously, we were interested in the effect of a firm having its knowledge stolen—so the relevant treatment event is when a targeted firm is compromised and its information is leaked to a competitor. However, we cannot interpret firm actions as endogenous responses unless the targeted firm is *aware* that they have been targeted. As a result, the important event is when a firm *discovers* that they have been targeted for espionage. As Figure 1 shows, there is substantial variation in how long espionage lasts. Sometimes there are years between when a company is first compromised and when espionage ends, other times the espionage is a one-time event and so there is no distinction. The date of espionage ending is our best proxy for when a firm discovers that it has been targeted for espionage.

is consistent with the overall declines in firm size, spending on R&D, and number of scientists employed that we document above, and may represent a substantial loss of knowledge given the frontier research that these firms tend to engage in.

However, it's important to distinguish between a reduction in patenting because firms are being less innovative, and a reduction in patenting because firms are being more secretive about the technologies they are developing. Only the latter contributes to a reduction in knowledge diffusion. We proxy for this measure of "secrecy" with the patents filed per dollar of R&D expenditure—reflecting the fact that if the results of R&D are being held as trade secrets, that would result in a fall in patents filed per R&D dollar. Thus, in Panel B we estimate how espionage affects the patent-to-R&D ratio. The results show that if anything, espionage increases the patent-R&D ratio. For firms to have become more secretive, they would have had to become much more efficient in converting R&D spending into real innovation, which is unlikely given the other measures of firm decline. Thus, we do not see firms becoming less likely to share knowledge through patenting after being targeted for espionage.

Consistent with this surprising result, we find no evidence of firms restricting their international collaborations in the rest of the panels in Figure 7. Firms are no less likely to patent with inventors living in China (Panel C), or inventors living outside the US (Panel D), conditional on patenting at all. The innovation literature also uses patent citations as an indicator of knowledge diffusion—in Panels E and F, we show that citations to the targeted firm's patents also do not change in response to espionage, nor does the share of those citations from Chinese firms decrease. This indicates that targeted firms do not seem to restrict other firms' awareness of their technologies.

Collectively, these results indicate that targeted firms do not deliberately make their patented technologies less open to China or the rest of the world. This implies that firms do not view patented technologies as providing a large source of espionage risk, relative to the benefits they get from patenting and having a certain set of inventors.

5.2 Employee Screening

The key vector for espionage is employees of the targeted firm. Thus, an important margin of response for targeted firms is how to adjust their employment decisions. In particular, do firms become more discriminatory towards employees who they perceive as "high espionage risk"? In espionage cases involving China, the most likely category that firms would want to restrict is ethnically Chinese employees—especially

those doing deep technical work that they could take to Chinese firms. This kind of employment discrimination would be illegal, but is certainly a plausible response by firms.

To test whether this happens, we use the LinkedIn data provided by Revelio Labs, with two additional features estimated by Revelio from the raw LinkedIn data. The first feature is that while Revelio anonymizes the raw LinkedIn data, they do classify employees into ethnic categories based on their name. Thus, we can observe the number of ethnically Asian employees at each firm over time. This is of course not a perfect proxy for espionage risk, as it covers many non-Chinese employees. Nonetheless, it is the best proxy we have, since we do not have the names of individuals in our data.

The second feature is that Revelio classifies job titles into 1500 employment categories, which we manually classify to determine whether a job involves R&D work (e.g. "process development engineer", "research scientist"). Since scientific employees possess the most technical knowledge, they are the most plausible vectors of espionage.

In Figure 8, we test whether employment of ethnically Asian workers falls differentially in targeted firms, where employment is measured as the stock of workers from the LinkedIn data. Panel A shows that while firms see 40% lower employment after espionage incidents (consistent with the overall decline in firm revenue), this decline is uniform for Asian and non-Asian employees. However, focusing on scientists, Panel B tells a slightly different story—the number of non-Asian scientists falls by 30% five years after an espionage incident, but the number of Asian scientists falls by 50%. A joint test of significance shows that the coefficients are marginally different (p=0.068).

This result—that targeted firms see differential declines in their employment of Asian scientists vs non-Asian scientists—bears closer examination. Does it reflect discrimination against Asian scientists? Or is it because they have better outside options, and so they are better able to jump off a sinking ship?

We can answer this question using imputed salary and seniority measures from Revelio Labs. In addition to the raw LinkedIn data that we have used so far, Revelio imputes a measure of salary and seniority for each worker. Salary measures are imputed from other data covering job postings for the role currently occupied by that worker. Seniority is imputed through an ensemble model that combines information from an employee's current job title, company, industry, job history, and other characteristics. These are binned into a seven point scale, when 1 represents entry level jobs (ex. accounting intern, paralegal), 4 represents manager level jobs (ex. account manager,

lead lawyer), and 7 a senior executive job (ex. CEO, CFO).[10] Then we can estimate an event-study at the *individual* level, where the treatment $D_{i,t}$ is now whether scientist i was at a firm that was targeted at time t or earlier.

Figure 9 shows the career trajectories of scientists at targeted firms, split by whether they leave the firm or not. Across Panel A.1 and A.2, departing Asian scientists leave to more senior positions while staying Asian scientists see a slowdown (although both effects are noisy)—in contrast, non-Asian employees see no changes to seniority regardless of moving or staying. This suggests differential selection pressures for Asian and non-Asian scientists after an espionage incident. Similarly, both Asian and non-Asian scientists see salary reductions, but the reductions are twice as large for Asian scientists.

Could this just be adverse selection, where the best Asian scientists are leaving for better jobs and the worst are staying and stagnating? Although possible, this does not explain why the same pattern does not appear for non-Asian scientists (the difference between Asians and non-Asians is often slightly short of statistically significant, $p \in (0.1, 0.2)$). While we cannot confirm statistically that the selection patterns for Asians and non-Asians are different, they are suggestive. Thus, while the evidence suggests discrimination as a potential explanation of the results, we acknowledge that it is imprecisely measured.

Taken together, these findings suggest that firms endogenously respond to espionage incidents. Our evidence suggests that targeted firms do not necessarily become more secretive by keep more trade secrets and patenting less of their innovation, or by the global collaboration and diffusion of their patents. Rather, it is their treatment of specific employees, such as Asian scientists, that changes in response to espionage, with these employees facing steeper career penalties within these firms and being likelier to ultimately leave these firms. The allocation of scientific talent is shifting in response to geopolitical tensions, a pattern which may persist in the future.

[10] It is important to emphasize the limitations of the outcome data here. Both seniority and salary are imputed by Revelio Labs rather than observed as ground truth. These imputations are difficult to audit for concerns that could confound these results. This is why we use these outcomes only to interpret the result that targeted firms see a differential reduction in their number of Asian scientists.

6 Conclusion

This paper provides evidence on how economic espionage shapes knowledge flows between the US and China in an era of geopolitical rivalry. We show that economic espionage has substantial negative effects on targeted firms, with revenues and R&D expenditures declining by roughly 20% within three years. These firm-level effects translate into aggregate effects—Chinese exports in targeted sectors rise by roughly 60% over a decade, while US exports decline by a similar amount, with a negative net effect on global trade. These results point to consequences of espionage not being restricted to the targeted firms.

Perhaps surprisingly, we find little evidence that firms respond to espionage by deliberately restricting their knowledge flows to China or the rest of the world. While targeted firms patent less overall, conditional on patenting, they are no less likely to patent with inventors in China, patent with ethnically Chinese inventors, or have their patents cited by Chinese firms. However, they do differentially reduce their employment of ethnically Asian scientists, with their employment of Asian scientists falling by roughly 50% compared to a 25% decline in overall scientist employment.

These findings have important implications for how we think about knowledge flows in an era of US-China strategic rivalry. First, they suggest that economic espionage represents a meaningful transfer of knowledge and competitive advantage from US to Chinese firms, rather than just unsuccessful attempts at technology theft. Second, the lack of responses by firms to restrict knowledge flows in response to espionage suggests that the benefits of international knowledge sharing may outweigh the risks of technology theft for many companies. Knowledge diffusion will likely continue to occur even as it becomes more politically charged.

Several important questions remain for future research. First, our results raise the question of why firms do not appear to restrict knowledge flows in response to espionage. One possibility is that these sectors are already heavily regulated, such that marginal restrictions on knowledge are actually difficult. Another possibility is that the knowledge flows embodied in patents pose very little espionage risk to firms, whereas the knowledge possessed by scientists is much more valuable to restrict.

Second, while we have compiled the most comprehensive dataset on economic espionage that we are aware of, our dataset represents only the tip of the iceberg when it comes to economic espionage. Future research could use confidential data from security firms or governments to gain a more representative picture of economic espionage

events, and be able to make more confident claims about the typical espionage case than we can in our setting.

Finally, much knowledge diffusion, both licit and illicit, happens through the movement of workers. Future research could examine the movement of workers between American and Chinese companies to understand the knowledge diffusion embodied in these moves. While our paper is about the harms from economic espionage, it is not an accounting of any costs and benefits associated with the movement of knowledge workers across countries, and such movement can be tremendously beneficial for both countries.

References

[1] Ufuk Akcigit and Sina T Ates. "What happened to US business dynamism?" In: *Journal of Political Economy* 131.8 (2023), pp. 2059–2124.

[2] Dmitri Alperovitch et al. *Revealed: operation shady RAT*. Vol. 3. McAfee, 2011.

[3] Francisco J Buera and Ezra Oberfield. "The global diffusion of ideas". In: *Econometrica* 88.1 (2020), pp. 83–114.

[4] Christopher Clayton, Matteo Maggiori, and Jesse Schreger. *A framework for geoeconomics*. Tech. rep. National Bureau of Economic Research, 2023.

[5] Filippo Curti et al. "Stolen Secrets: The Effect of Trade Secret Theft on Corporate Innovation". In: *Available at SSRN* (2023).

[6] DOJ. "Trade Secrets to Competitors in China". In: (Jan. 2015). Accessed on Jan 15, 2025. URL: https://www.justice.gov/sites/default/files/nsd/pages/attachments/2015/01/23/export-case-list-201501.pdf.

[7] Jonathan Eaton and Samuel Kortum. "International technology diffusion: Theory and measurement". In: *International Economic Review* 40.3 (1999), pp. 537–570.

[8] Hanming Fang and Ming Li. *Red Scare? A Study of Ethnic Prejudice in the Prosecutions under the Economic Espionage Act*. Tech. rep. National Bureau of Economic Research, 2021.

[9] FBI. "Chinese Talent Plans". In: (Nov. 2020). Accessed on Jan 15, 2025. URL: https://web.archive.org/web/20201117085251/https://www.fbi.gov/investigate/counterintelligence/the-china-threat/chinese-talent-plans.

[10] FBI. "Former Paint Manufacturing Chemist Sentenced to 15 Months in Prison for Stealing Trade Secrets Valued up to 20*Million*". In: (Dec. 2010). Accessed on Jan 15, 2025. URL: https://archives.fbi.gov/archives/chicago/press-releases/2010/cg120810-1.htm.

[11] Robert Flynn et al. *Building a wall around science: The effect of US-China tensions on international scientific research*. Tech. rep. National Bureau of Economic Research, 2024.

[12] María García-Vega and Elena Huergo. "Determinants of international R&D outsourcing: the role of trade". In: *Review of Development Economics* 15.1 (2011), pp. 93–107.

[13] Albrecht Glitz and Erik Meyersson. "Industrial espionage and productivity". In: *American Economic Review* 110.4 (2020), pp. 1055–1103.

[14] Eileen Guo, Jess Aloe, and Karen Hao. "The US Crackdown on Chinese Economic Espionage is a Mess. We Have the Data to Show It". In: *MIT Technology Review* (Dec. 2021). URL: https://www.technologyreview.com/2021/12/02/1040656/china-initative-us-justice-department/.

[15] Thomas J Holmes, Ellen R McGrattan, and Edward C Prescott. "Quid pro quo: Technology capital transfers for market access in China". In: *The Review of Economic Studies* 82.3 (2015), pp. 1154–1193.

[16] DA Hounshell. *Science and Corporate Strategy: Du Pont R&D, 1902-1980*. Cambridge University Press, 1988.

[17] Mara Hvistendahl. *The Scientist and the spy: A true story of China, the FBI, and industrial espionage*. Penguin, 2021.

[18] Ruixue Jia et al. *The impact of US-China tensions on US science*. Tech. rep. National Bureau of Economic Research, 2022.

[19] Andrew Chongseh Kim. "Prosecuting Chinese Spies: An empirical analysis of the economic espionage act". In: *Cardozo L. Rev.* 40 (2018), p. 749.

[20] Tor Jakob Klette and Samuel Kortum. "Innovating firms and aggregate innovation". In: *Journal of political economy* 112.5 (2004), pp. 986–1018.

[21] Chris Miller. *Chip war: The fight for the world's most critical technology*. Simon and Schuster, 2022.

[22] Alex Nowrasteh. "Espionage, Espionage-Related Crimes, and Immigration: A Risk Analysis, 1990-2019". In: (2021).

[23] Justin R Pierce and Peter K Schott. "A concordance between ten-digit US Harmonized System Codes and SIC/NAICS product classes and industries". In: *Journal of Economic and Social Measurement* 37.1-2 (2012), pp. 61–96.

[24] Shawn Rostker et al. *Survey of Chinese Espionage in the United States Since 2000*. https://www.csis.org/programs/strategic-technologies-program/survey-chinese-espionage-united-states-2000. 2023.

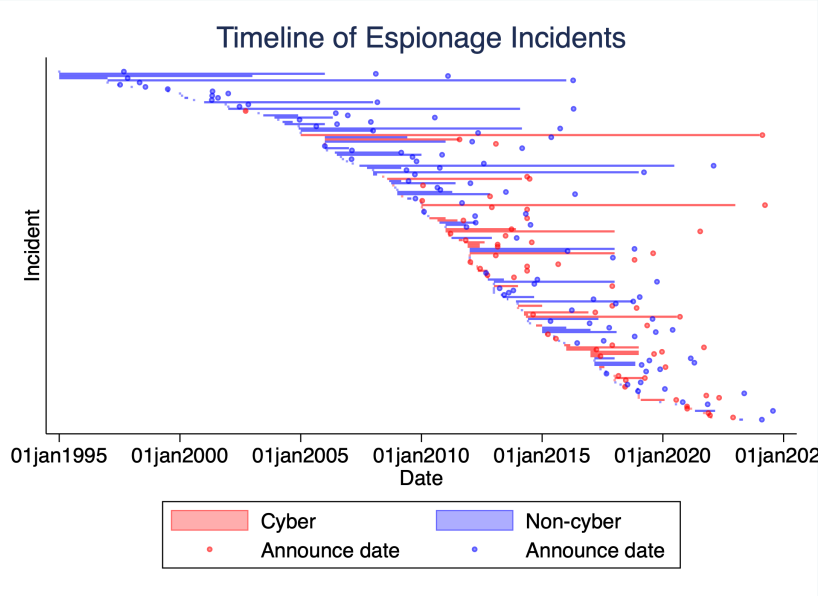
[25] New York Times. "Air France Denies Spying on Travelers". In: *The New York Times* (Sept. 1991). Accessed on Jan 6, 2025. URL: https://web.archive.org/web/20151016000311/http://www.nytimes.com/1991/09/14/news/14iht-spy_.html?pagewanted=1.

[26] New York Times. "U.S. Drops Its Case Against M.I.T. Scientist Accused of Hiding China Links". In: (Jan. 2022). Accessed on Jan 15, 2025. URL: https://www.nytimes.com/2022/01/20/science/gang-chen-mit-china-initiative.html.

[27] Jeremy S. Wu. *Federal Cases*. https://jeremy-wu.info/?page_id=1088. 2024.

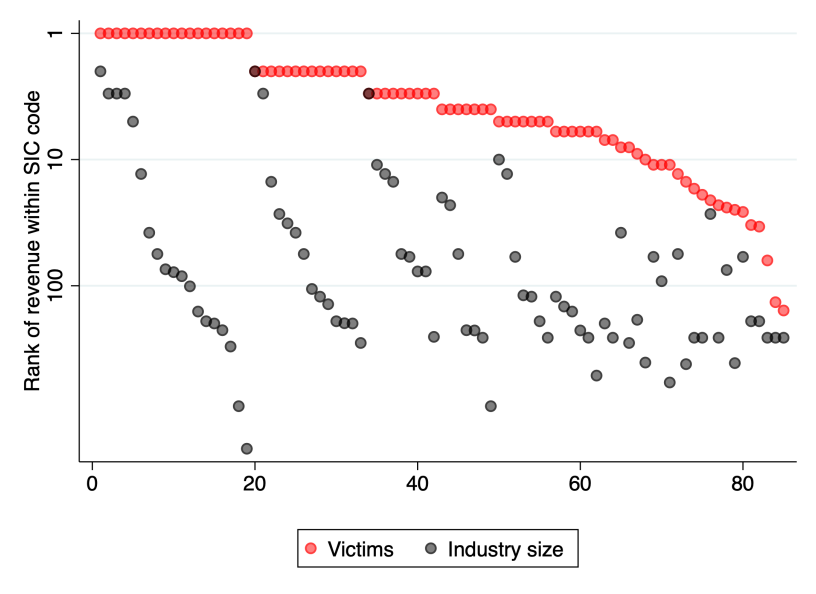
7 Figures and Tables

Figure 1: Timeline of espionage incidents



Note: This figure presents a timeline of economic espionage incidents against firms in the United States since 1995. Each row contains a separate incident. The shaded bars span the duration in which espionage occurs (the beginning of the bar corresponds to when espionage began, and the ends of the bar correspond to when the proprietary information was last successfully extracted, or when the suspect was caught if they were caught). The announcement date indicates the date in which the espionage incident was first announced to the public. Incidents that are primarily cyber in nature are plotted in red, while non-cyber incidents are plotted in blue.

Figure 2: Rank of victim firms by revenue in industry

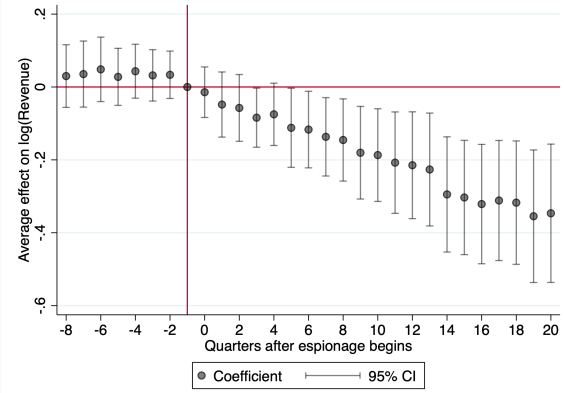


Note: This figure plots the rank of victim firm revenue within their industry (SIC code) in red, and the size of their industry in gray. Firms are ordered by rank, and then industry size. The y-axis uses a log-scale. Revenue is calculated as the average value prior to an espionage incident taking place.

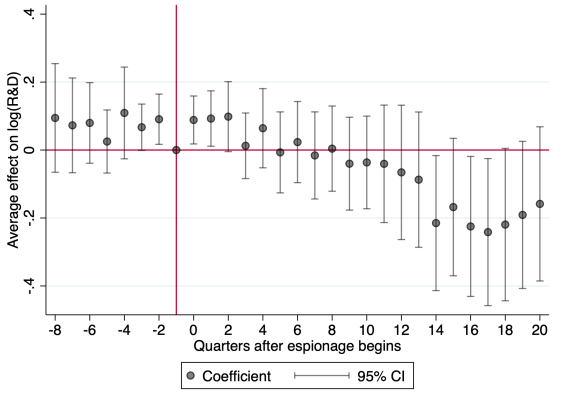
Figure 3: Effect of espionage on victim firm's log revenue and R&D expenditures

Panel A: Successful cases

Panel A.1: log(Revenue)

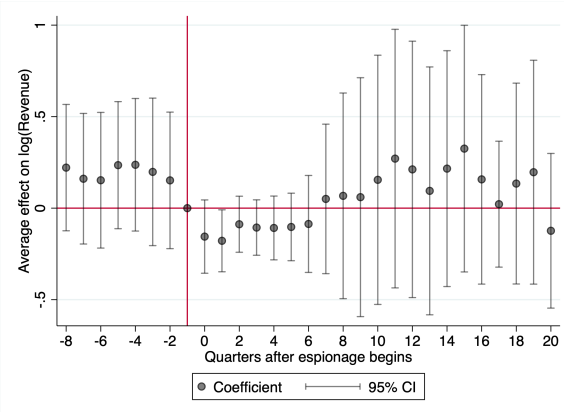


Panel A.2: log(R&D)

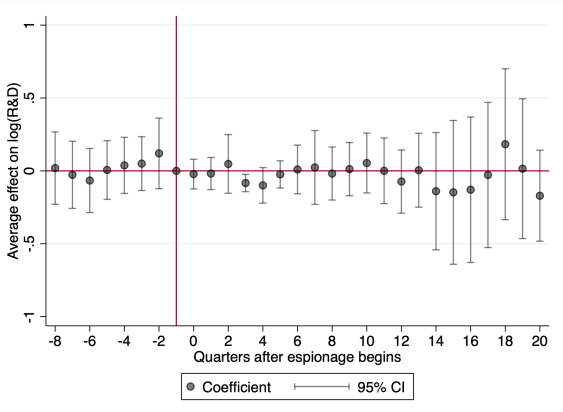


Panel B: Unsuccessful cases

Panel B.1: log(Revenue)

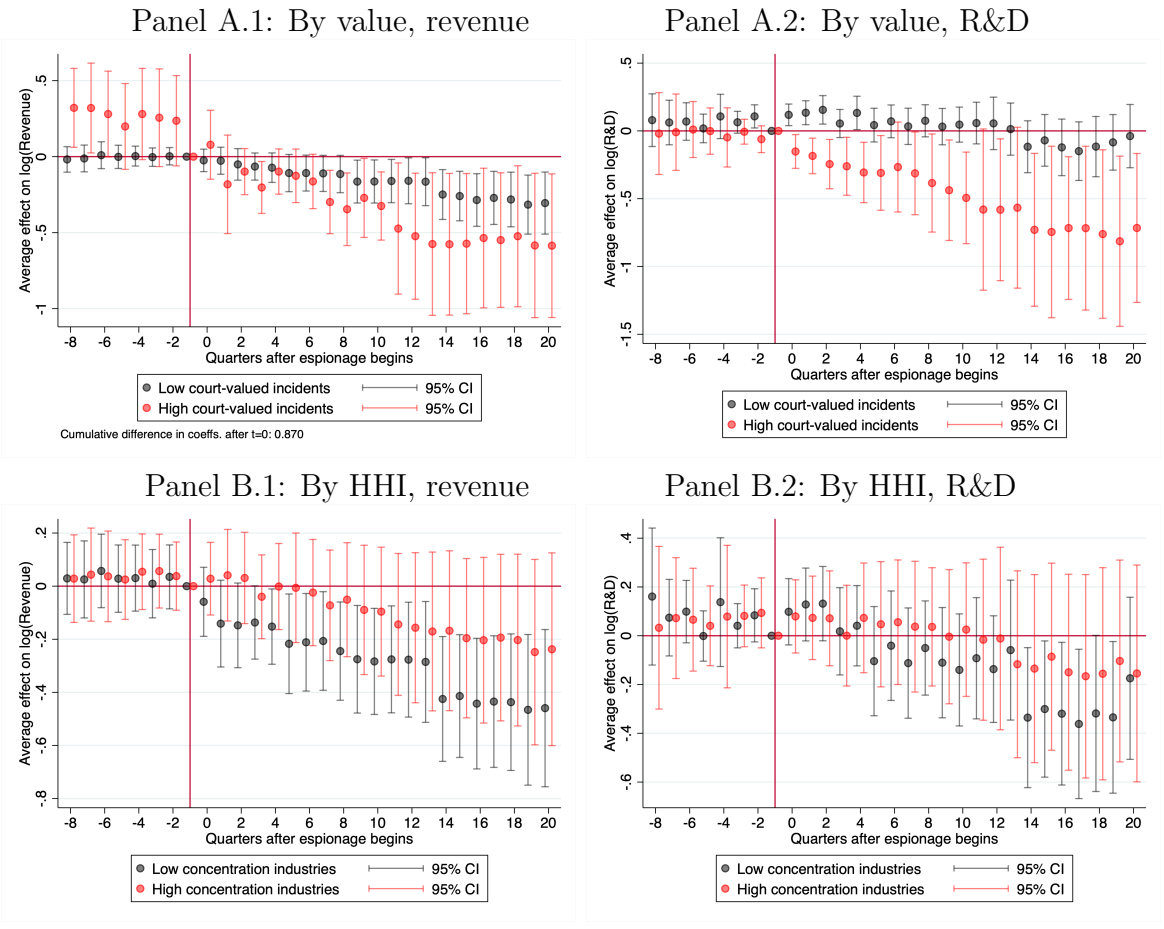


Panel B.2: log(R&D)



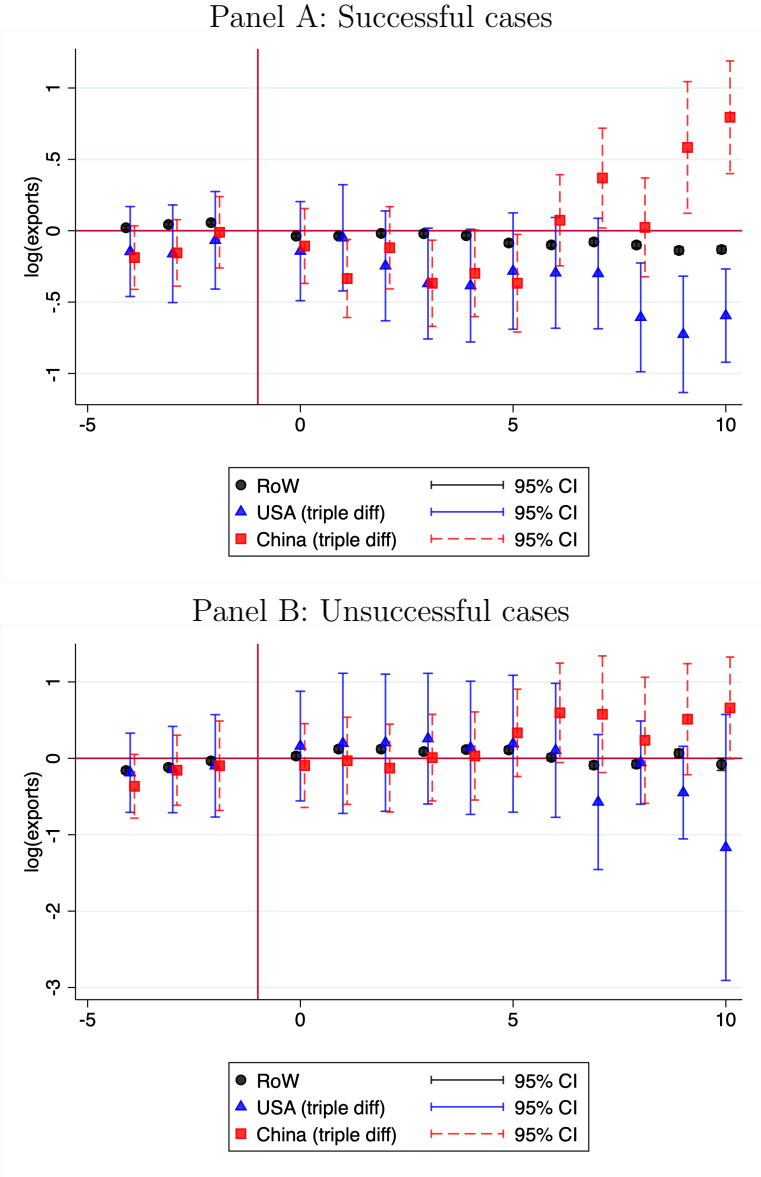
Note: This figure plots coefficients and 95% confidence intervals from a two-way fixed effects event study regression. In Panel A, an event is a firm being successfully targeted for economic espionage. In Panel B, events are unsuccessful cases of economic espionage, where the desired information was not successfully given to its intended recipient. The outcome in Panels A.1 and B.1 is a firm's log(Revenue) and in Panels A.2 and B.2, a firm's log(R&D expenditures). Standard errors are clustered at the firm level.

Figure 4: Heterogeneous effects of espionage



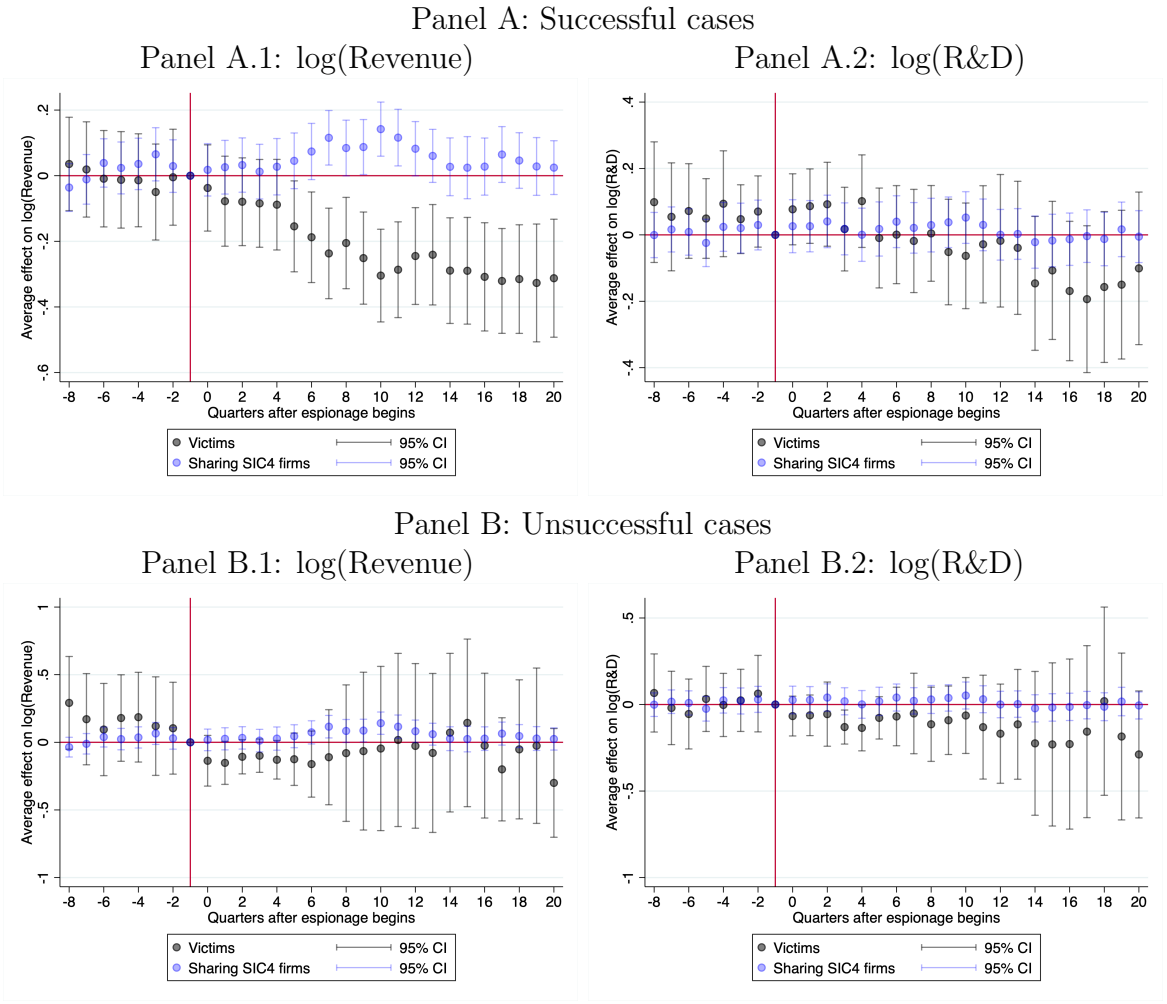
Note: This figure plots heterogeneous effects of espionage incidents. Panel A cuts cases by whether the claimed value of damages in court was above or below the median claimed damage. Panel B cuts cases by whether the targeted firm's industry HHI is above or below the median HHI across industries.

Figure 5: Effect of espionage on country-level exports



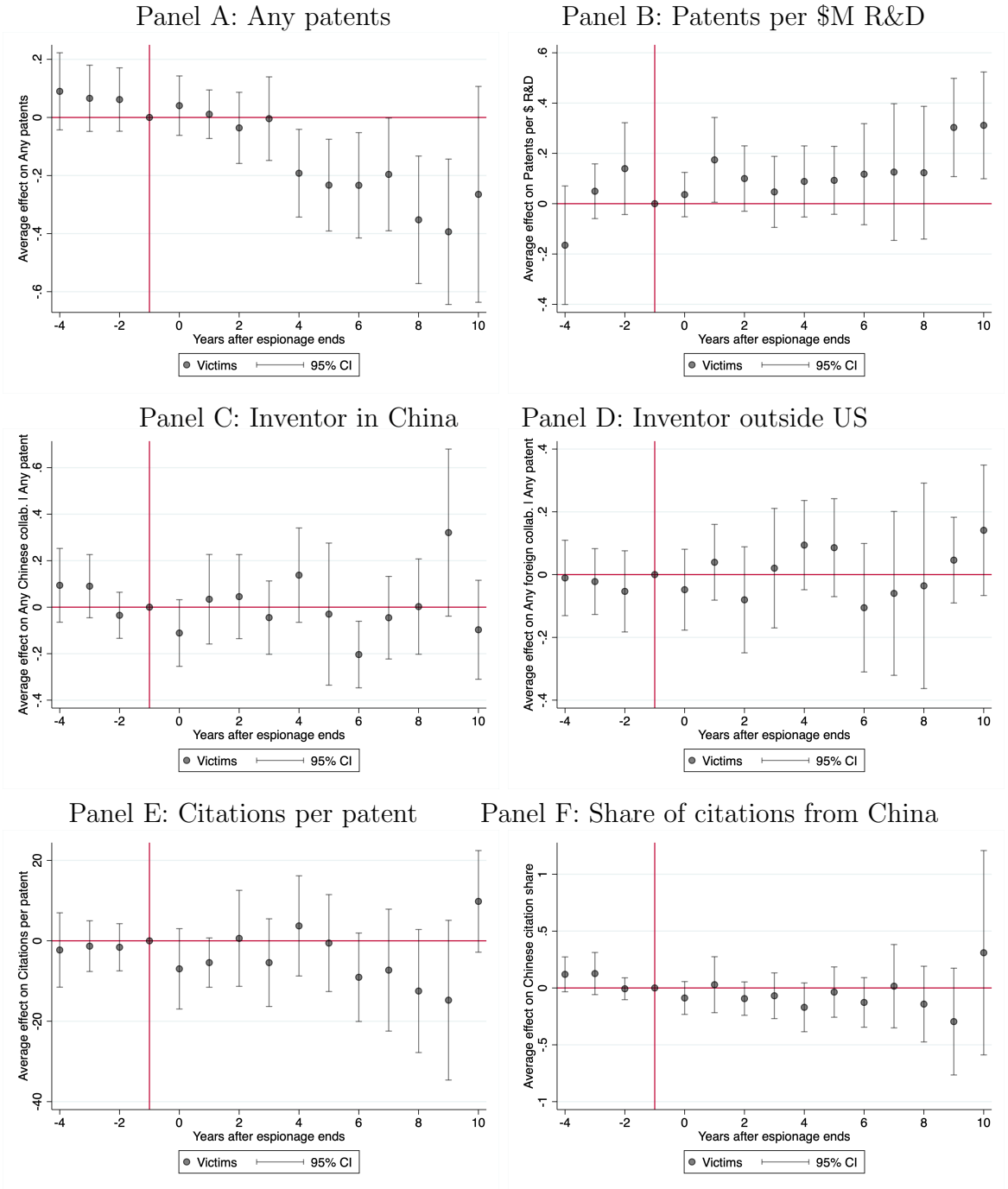
Note: This figure plots coefficients and 95% confidence intervals from a triple differences event study regression at the exporter-year-HS code level. The outcome is the total exports by the exporter in a given year and HS-6 code. The specification includes exporter-year and exporter-HS fixed effects. Coefficients for event-time indicators are plotted in black, while triple difference coefficients for the United States and China are plotted in blue and red respectively. Panel A restricts to successful attempts at espionage, while Panel B restricts to unsuccessful attempts as a placebo test. Standard errors are clustered at the exporter-HS level.

Figure 6: Effect of espionage on victims and other firms in the same industry, log revenue and R&D expenditures



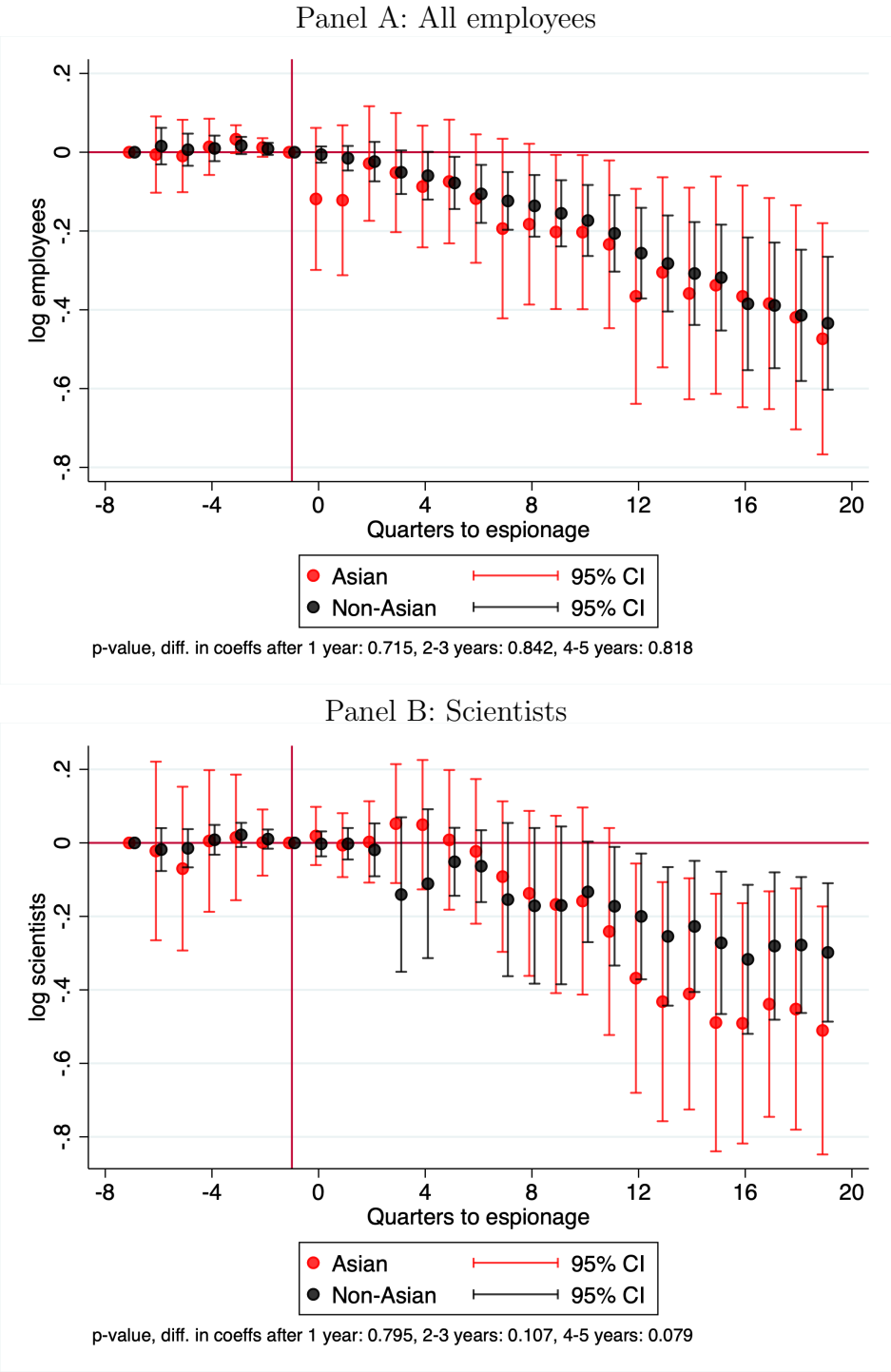
Note: This figure plots coefficients and 95% confidence intervals from a triple difference two-way fixed effects event study regression. In Panel A, an event is the first time an industry is successfully targeted for economic espionage. In Panel B, events are unsuccessful cases of economic espionage, where the desired information was not successfully given to its intended recipient. The outcome in Panels A.1 and B.1 is a firm's log(Revenue) and in Panels A.2 and B.2, a firm's log(R&D expenditures). The sample consists of all firms in treated industries (SIC-4 codes ever targeted for espionage) and "nearby" never-treated industries (industries sharing an SIC-3 code with treated SIC-4 industries). Coefficients for event-time indicators are plotted in blue, while triple difference coefficients for victim firms are plotted in black. Standard errors are clustered at the firm level.

Figure 7: Effect of espionage on patent-based foreign collaboration



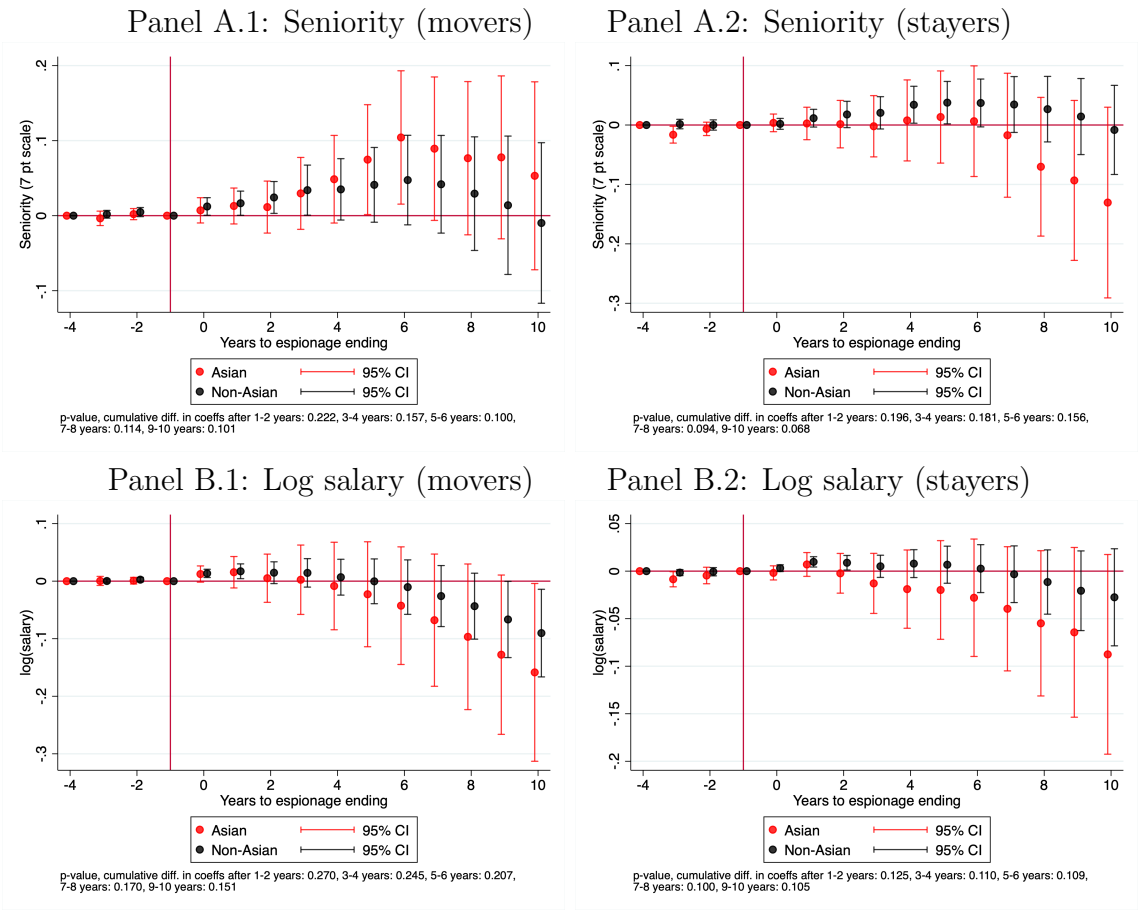
Note: This figure plots coefficients and 95% confidence intervals from two-way fixed effects regressions. An event is when an successful economic espionage incident ends. The outcome in Panel A is whether the firm patented in a given year, in Panel B the number of patents per million dollars of R&D expenditures, in Panel C whether the firm had a patent with an inventor living in China, in Panel D whether the firm patented with an inventor outside the US, in Panel E how many citations each patent by the firm receives, in Panel F what share of those citations are from Chinese firms. Inventor location is inferred from the address on a patent application. Panels C-F measure outcomes conditional on the firm filing any patent at all. Standard errors are clustered at the firm level.

Figure 8: Effect of espionage on employment by race



Note: This figure plots coefficients and 95% confidence intervals from two-way fixed effects regressions. An event is when an successful economic espionage incident ends. The outcome in Panel A is the log(employees) and in Panel B the log(scientists) employed by the firm belonging to each racial background. Plotted in red are coefficient estimates for Asians and in black, coefficient estimates for non-Asians. Standard errors are clustered at the firm level.

Figure 9: Career trajectories for scientists at targeted firms



Note: This figure plots descriptive event-study regressions at the worker level, using data from LinkedIn. Each unit is a worker with a job title that focuses on scientific work, and treatment is determined by being at a firm targeted for espionage. Seniority is imputed by Revelio Labs using an employee's current job title, company, industry, and job history. A worker's salary is imputed by Revelio Labs from other data covering job postings for the role currently occupied by that worker. A firm is classified as young if it is less than 10 years old in LinkedIn data. Standard errors are clustered at the firm level.

Table 1: Industries targeted for espionage more than once

SIC	Industry name	Times targeted
(1)	(2)	(3)
3674	SEMICONDUCTORS & RELATED DEVICES	10
2820	PLASTIC MATERIAL, SYNTH RESIN/RUBBER, CELLULOS (NO GLASS)	6
2851	PAINTS, VARNISHES, LACQUERS, ENAMELS & ALLIED PRODS	5
2834	PHARMACEUTICAL PREPARATIONS	4
3812	SEARCH, DETECTION, NAVAGATION, GUIDANCE, AERONAUTICAL SYS	4
3663	RADIO & TV BROADCASTING & COMMUNICATIONS EQUIPMENT	3
3711	MOTOR VEHICLES & PASSENGER CAR BODIES	3
7370	SERVICES-COMPUTER PROGRAMMING, DATA PROCESSING, ETC.	3
100	AGRICULTURAL PRODUCTION-CROPS	2
1311	CRUDE PETROLEUM & NATURAL GAS	2
2086	BOTTLED & CANNED SOFT DRINKS & CARBONATED WATERS	2
2860	INDUSTRIAL ORGANIC CHEMICALS	2
2911	PETROLEUM REFINING	2
3721	AIRCRAFT	2
3724	AIRCRAFT ENGINES & ENGINE PARTS	2
3845	ELECTROMEDICAL & ELECTROTHERAPEUTIC APPARATUS	2
4812	RADIOTELEPHONE COMMUNICATIONS	2

Note: This table presents captures all sectors targeted more than once. Column 1 presents the SIC-4 code, column 2 a description of the industry, and column 3 the number of times it was targeted for espionage.

Online Appendix

This appendix contains additional material, including figures and tables.

Appendix A Additional Analysis

Appendix A.1 Effects on Targeted Firms

Alternative Design: Matching on Industry Dynamics Our main specification compares targeted and non-targeted firms in the same industry. However, Figure 2 shows that firms that are targeted for espionage overwhelmingly tend to be leaders in their field—more than half of targeted firms are in the top 3 firms in their industry when they are targeted, often in very large industries. This fact raises concerns that our main specification could be confounded by industry dynamics; if espionage has no effect, but leader firms naturally decline compared to other firms in the same sector, then we might estimate that espionage has negative effects simply because of this mean reversion. To address this concern, in Figure A.11, we show that industry leaders do not systematically mean-revert, especially when we focus on firms targeted by espionage.[1]

However, other more complex business dynamics may exist, including industry-specific patterns of churn, or time-and-industry specific shocks that only affect leaders. To address these broad classes of concerns, we also consider a complementary specification, based on matching targeted firms to similar firms in nearby industries (i.e. in the same SIC 3-digit code, but not in the same SIC 4-digit code). This matching is done based on factors that capture industry dynamics.[2] The estimating equation is

$$y_{i,t} = \sum_{k=-8}^{20} \gamma_k D_{i,t+k} + \alpha_i + \alpha_{m(i),t} + \varepsilon_{i,t} \tag{5}$$

where $m(i)$ is a matched pair group that contains one victim firm and the closest SIC-3 firm that is matched to the victim firm. We replace the industry-quarter fixed effects with matched pair-quarter fixed effects, to control for any dynamics that industry leaders may be exposed to at each point in time. This alternative design essentially differences out any possible industry dynamics that could confound our results. In Table A.1, we test whether industries targeted by espionage exhibit similar dynamics to SIC-3 industries, and find that they are comparable, with no statistically significant

[1] Industry leadership is highly autocorrelated, and the average leader firm targeted by espionage has already been a leader for over 15 quarters by the time they are targeted.

[2] Specifically, we match targeted firms to the nearest firms based on the L2 Minkowski distance on industry rank at $t = -1$, industry rank at $t = -8$, whether a firm is in the top 3 industry firms at $t = -1$, and time spent in the top 3 firms as of $t = -1$, where $t = 0$ is the period in which espionage begins.

differences in the persistence of industry leadership (columns 1-4), size difference between top firms (column 5), or HHI (column 6) between them. This justifies the choice of firms in nearby SIC industries as a comparison group to eliminate the effect of any industry dynamics.

The results of estimating the matched pair design in Equation 5 are given in Figure A.2. Reassuringly, even with this different specification, we find results consistent with our main specification. The effects on firm revenue are quicker to appear and larger in magnitude than in our main specification—a year after espionage begins, targeted firms have 50% lower revenues than similar firms in other industries. The effects on R&D expenditures are smaller but still significant, with targeted firms having 10-20% lower R&D expenditures than similar firms in other industries 5 years after espionage begins. Thus, our results go through under an alternative design that exploits different variation.

This alternative design differences out industry dynamics that could confound our results and also increases precision by comparing targeted firms to firms that are similar. However, we lose the ability to include industry-by-time FEs, so that selection of industries into being targeted for espionage could now confound our results. We find no evidence of this selection in the pre-trends of the matched event study—nonetheless, we use this design as a complement to our main specification, and treat consistency between them as evidence that our results are robust.

Robustness Checks To complement the placebo test and the matched-pair estimator, we conduct two other robustness checks. First, we see whether alternative difference-in-difference estimators yield different results from the baseline specification in Equation 1. In Figure A.3, we plot dynamic treatment effects under a variety of alternate estimators and show that results are not sensitive to the choice of estimator. This is natural, because recent event study estimators vary primarily in how they compare units treated at different times. However, in our setting, most firms in our data are never treated. As a result, most of the identifying comparisons are between ever-treated and never-treated firms, which the TWFE estimator and more recent event study estimators handle similarly. Therefore, for the rest of the paper we report results only from the TWFE estimator in Equation 1.

The second robustness check is about measurement error. One may be concerned that our coding of the timing of espionage may be subject to measurement error—although we are usually able to identify the month in which espionage began, in roughly 30% of cases we only have precision at the annual level. In Figure A.4, we re-estimate Equation 1 at the year level and show that our headline findings remain unchanged. The longer time horizon also shows that the effects of espionage are persistent even a decade after the incident and do not fade out over time.[3]

[3]Whenever there is ambiguity on the timing of events, we take the earliest possible date to avoid contaminating the pre-trend. This comes at the risk of estimating a more delayed effect of espionage.

Secondary Outcomes While revenues and R&D expenditures are flow quantities, one can also test whether their stock analogues, total assets and intangible assets, are affected by espionage. In Figure A.5, Panels A and B, we find that economic espionage has a negative effect on a firm's total assets and intangible assets. We once again find a lack of pre-trends, and find that their path follows a similar pattern to revenues and R&D, declining by 20 to 30% within 3 years of espionage beginning, with effects persisting in the 2 years that follow. However, in Figure A.5, Panels C and D, we examine the impact of economic espionage on gross and net profit margins respectively. We find null effects, consistent with the interpretation that these firms are declining in scale, but not experiencing changes in mark-ups.

Using operating segment data from Compustat, we can also decompose these changes in firm revenues into differences by exports and domestic sales to see where firms are most affected by espionage. In Figure A.6, we show that domestic sales and exports both drop following economic espionage incidents. Roughly a decade after the espionage incident, a firm's exports have declined by roughly 70% relative to other firms in their industry, whereas domestic sales see a (slightly) more modest 50% decline.

Effects on Stock Returns To measure effects on firms that might not be captured by the balance sheet data, we examine the stock market response to espionage. To do this, we estimate each firm's *cumulative abnormal returns* at various time horizons using Fama-French factors.[4]

Figure A.7 displays these effects, for two definitions of treatment—when espionage begins (Panel A.1), and when espionage is announced (Panel A.2) We find that the declines in firm valuations also track the declines in firm fundamentals, with a roughly 20 to 30% drop in firm value two years after espionage begins. We interpret the initial drop in a firm's valuation as the market reacting to a fundamental decline in firm value due to espionage—most of the time, the public does not know that an espionage incident has occurred until after the 2 year window displayed.[5] The announcement of an espionage incident is associated with a further 20% penalty to firm valuation in the 2 years afterwards, although this likely combines the fundamental effect of espionage itself alongside any announcement effects. To narrow down the effect of announcement, we examine a firm's CAR in the days immediately surrounding the announcement in Figure A.12, Panel A. Estimates are noisy, but point towards a roughly 4% decline immediately upon announcement.

In Figure A.7, Panel B, we plot cumulative abnormal returns for firms that are victims of an unsuccessful espionage incident. We find that estimates are very noisy but positive. If those conducting espionage have any inside knowledge (for instance,

[4]Specifically, we regress daily returns on Fama-French factors for the pre-period for victim firms to obtain a firm's normal returns. We use these estimated coefficients to project normal returns and difference them from realized daily returns to obtain abnormal returns. We then sum over the days since the event occurred to obtain the cumulative abnormal return.

[5]The median (mean) gap between an espionage incident beginning and the public announcement of an incident is 2.2 years (over 3 years).

because they are employees of the victim firm), they are likely to target firms that are soon to outperform. This suggests that, if anything, the effects reported above may be underestimates. However, other interpretations are compatible with the rise in firm value, particularly after an unsuccessful espionage incident is announced: the market may take this as a signal that the firm has valuable technology (worthy of being stolen) or update on a firm's security capabilities.

Appendix A.2 Knowledge Diffusion Spillovers to Other Firms

Targeted firms are not the only firms that could endogenously respond to espionage. For example, Boeing might reduce its willingness to patent with Chinese inventors in response to espionage against Airbus. This is not just an independently important margin of response, it is an identification threat to the previous sections—by taking non-targeted firms as never-treated, we risk underestimating the endogenous response to espionage.

One way to estimate this aggregate margin of response would be to aggregate all of our outcome measures to the industry level, and estimate the effect of espionage in an industry. Unfortunately, industry-level data is too coarse to have any power, so we cannot run informative regressions at the industry-level. Thus, we instead follow the same approach as in Equation 4, where we assign treatment at the SIC 4-digit level, and we use firms in "nearby" SIC codes (i.e. same SIC 3-digit code but different SIC 4-digit code) as the never-treated group. For the employment outcomes, since Revelio Labs only provides NAICS codes and not SIC codes for firms in the LinkedIn data, we assign treatment at the NAICS 6-digit level, and we use firms in "nearby" NAICS 4-digit codes as the never-treated group. Just as with Equation 4, we only keep the first incident targeting an industry in estimation.

In Figure A.9, we estimate the spillover impacts of espionage to the employment of other firms in the industry. Panels A and B reveal that firms in industries targeted by espionage also appear to hire slightly fewer employees, in the 5-10% range, among both Asians and non-Asians.[6] On the other hand, Panels C and D reveal that the hiring of scientists *increases* slightly by 5-10% among both Asians and non-Asians. This suggests that firms do not necessarily update their hiring practices from the occurrence of espionage in other firms in their industry, whether along racial lines or across job categories.

In Figure A.10, we estimate the spillover impacts of espionage to patenting by other firms in the industry. Panel A shows that firms in industries targeted by espionage are about 5% more likely to file a patent, consistent with the small increases in the hiring of scientists that we observe. These slight increases are also found in patents involving Chinese or other foreign collaborators (Panels B-E), although they are imprecisely estimated. In Figure A.8, we examine the likelihood of patenting with Chinese or

[6]The estimates for victims become much more imprecise because NAICS 6-digit codes are relatively small, but estimated magnitudes are consistent with our prior estimates.

other foreign collaborators, conditional on patenting, and find largely insignificant results. Taken together with the results on employment, these results suggest that firms in industries targeted by espionage may try to increase their innovation activities—potentially to develop a lead over the stolen technology, or to outcompete the victim firm—but that they do not necessarily become less open to foreign collaboration and innovation.

One explanation for this non-response even at the industry level is that firms' decisions about optimal openness depend on their perception of espionage *risk*. As such, even if espionage makes them less open to knowledge flows, they might not respond to *individual events* of espionage. Indeed, given that many sectors are targeted repeatedly (Table 1) and thus presumably face a high background espionage risk, this is the natural interpretation to our null findings on the endogenous response of firms. However, our estimation only includes the first time an industry is targeted for espionage. Thus, as long as the *first* espionage incident in a sector updates firms' beliefs about espionage risk, our strategy should capture the responses of firms to espionage. The fact that we find no effects on other firms even from the first espionage incident in a sector implies that this is not simply an artifact of firms having generally well-calibrated beliefs about espionage.[7]

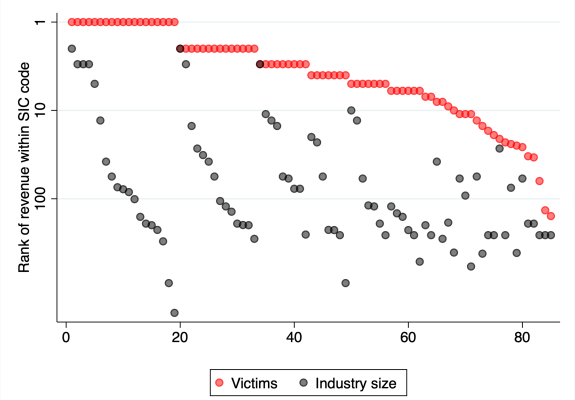
[7]However, we acknowledge a limitation of our data here; our data only covers publicly known cases. If firms are aware of earlier espionage cases in their industry that are not made public, then they could be not responding to espionage simply because they are already aware of the risk. This is a possibility that we cannot rule out with our data.

Appendix B Additional Tables and Figures

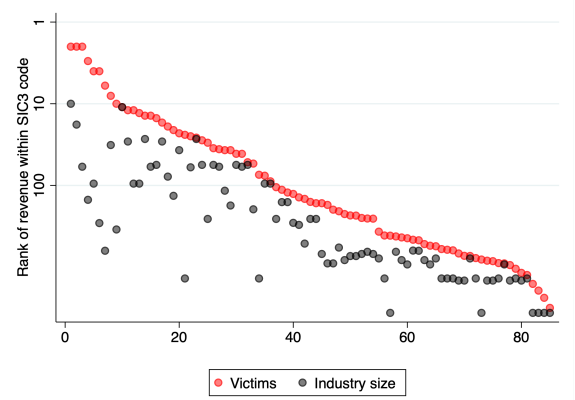
Figure A.1: Rank of victim firms by size within industry

Panel A: Revenue

Panel A.1: Industry is SIC

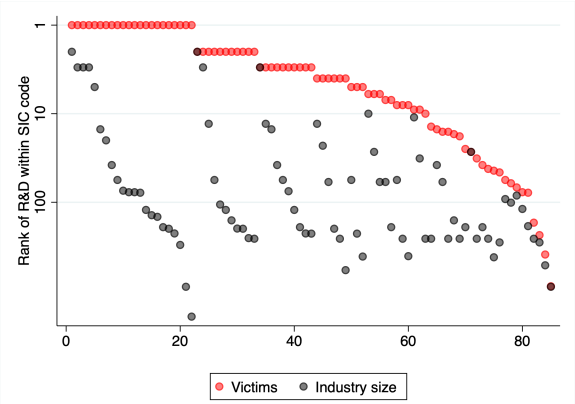


Panel A.2: Industry is SIC3

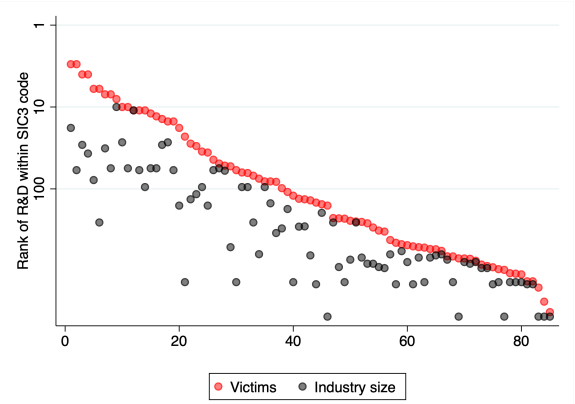


Panel B: R&D expenditures

Panel B.1: Industry is SIC

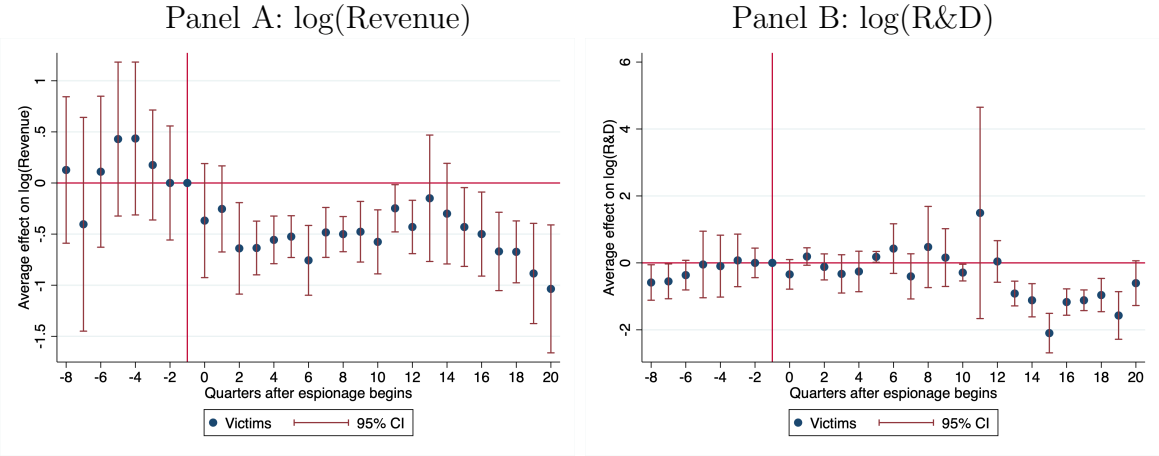


Panel B.2: Industry is SIC3



Note: This figure plots the rank of victim firms by size within their industry in red, and the size of their industry in gray. In Panels A and B, revenue is used as an indicator for firm size. In Panels C and D, R&D expenditures are used as an indicator for firm size. In Panels A and B, a firm's industry is defined as their SIC (4 digit) code. In Panels C and D, a firm's industry is defined at the SIC 3 digit code level. Firms are ordered by rank, and then industry size. The y-axis uses a log-scale. Revenue and R&D are both calculated as the average value prior to an espionage incident taking place.

Figure A.2: Effect of espionage on victim firm log revenue and R&D, matched pair design

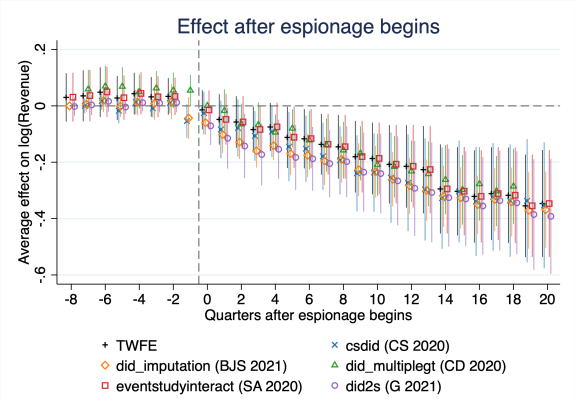


Note: This figure plots coefficients and 95% confidence intervals from a matched-pair event study regression. Each victim of a successful espionage incident is matched to the closest firm in a "nearby" industry (same SIC-3 but different SIC-4) based on time spent as industry leader and rank within industry based on revenue. An event is the victim firm in the match pair being successfully targeted for economic espionage. Specifications include match-pair by time and firm fixed effects. The outcome in Panel A is a firm's log(Revenue) and in Panel B a firm's log(R&D expenditures). Standard errors are clustered at the firm level.

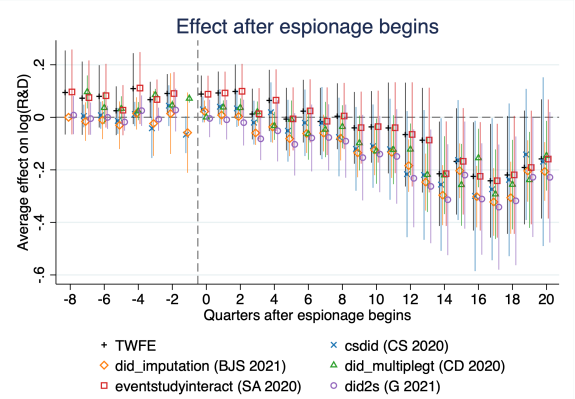
Figure A.3: Effect of espionage on victim firm's log revenue and R&D expenditures, alternate heterogeneous DID estimators

Panel A: Successful cases

Panel A.1: log(Revenue)

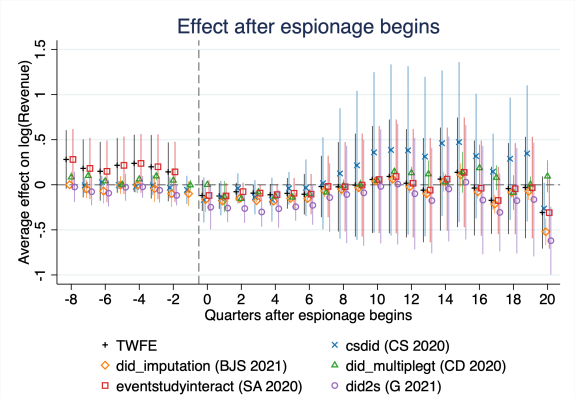


Panel A.2: log(R&D)

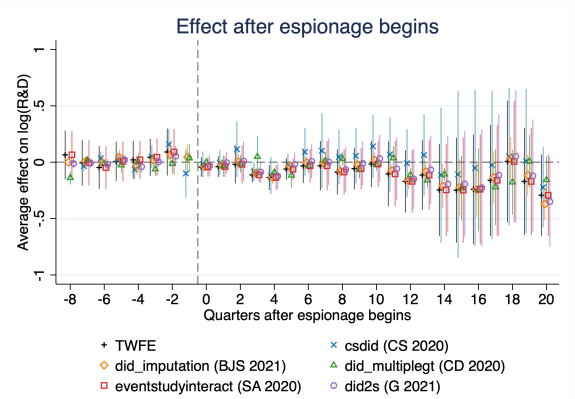


Panel B: Unsuccessful cases

Panel B.1: log(Revenue)



Panel B.2: log(R&D)

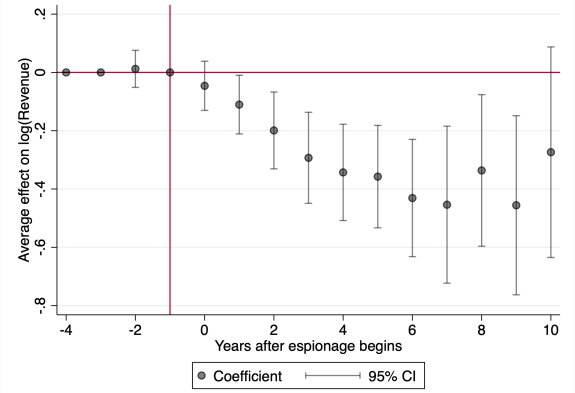


Note: This figure plots coefficients and 95% confidence intervals from various heterogeneous dynamic difference-in-difference specifications. In Panel A, an event is a firm being successfully targeted for economic espionage. In Panel B, events are unsuccessful cases of economic espionage, where the desired information was not successfully given to its intended recipient. The outcome in Panels A.1 and B.1 is a firm's log(Revenue) and in Panels A.2 and B.2, a firm's log(R&D expenditures). Black crosses present estimates from a standard two-way fixed effect design, blue crosses present estimates using Callaway and Sant'Anna (2021), orange diamonds present estimates using Borusyak, Jaravel, and Spiess (2023), green triangles present estimates using de Chaisemartrin and D'Haultfoeuille (2024), red squares present estimates using Sun and Abraham (2020), and purple circles present estimates using Gardner (2021). Standard errors are clustered at the firm level.

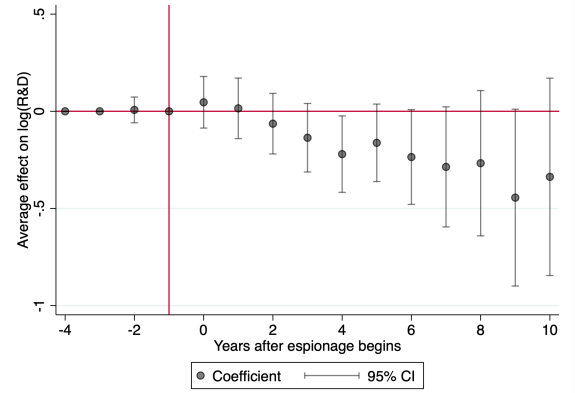
Figure A.4: Effect of espionage on victim firm's log revenue and R&D expenditures, time horizon of years

Panel A: Successful cases

Panel A.1: log(Revenue)

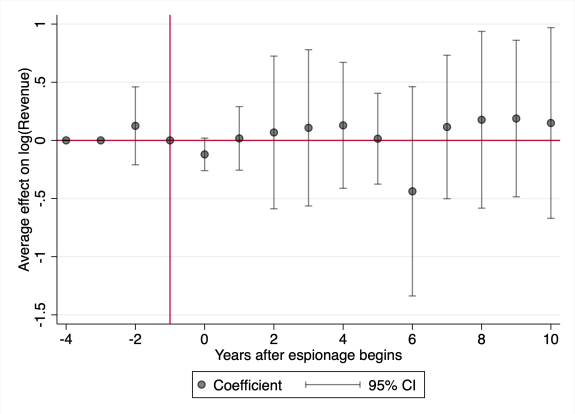


Panel A.2: log(R&D)

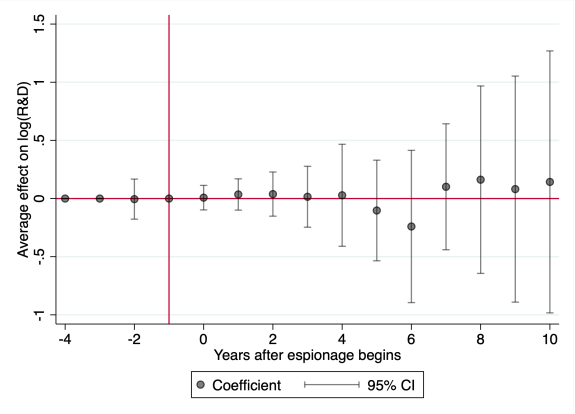


Panel B: Unsuccessful cases

Panel B.1: log(Revenue)



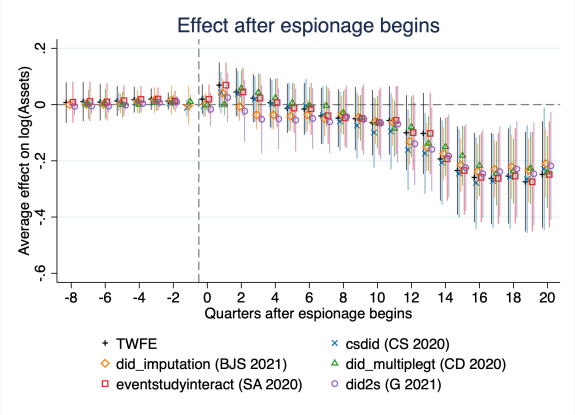
Panel B.2: log(R&D)



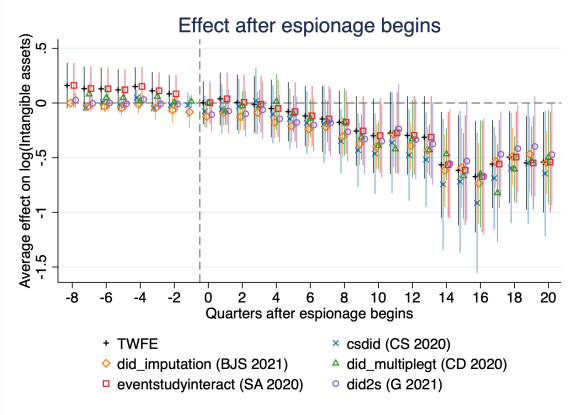
Note: This figure plots coefficients and 95% confidence intervals from a two-way fixed effects event study regression. In Panel A, an event is a firm being successfully targeted for economic espionage. In Panel B, events are unsuccessful cases of economic espionage, where the desired information was not successfully given to its intended recipient. The outcome in Panels A.1 and B.1 is a firm's log(Revenue) and in Panels A.2 and B.2, a firm's log(R&D expenditures). The unit of analysis is a firm by year. Standard errors are clustered at the firm level.

Figure A.5: Effect of espionage on secondary firm outcomes

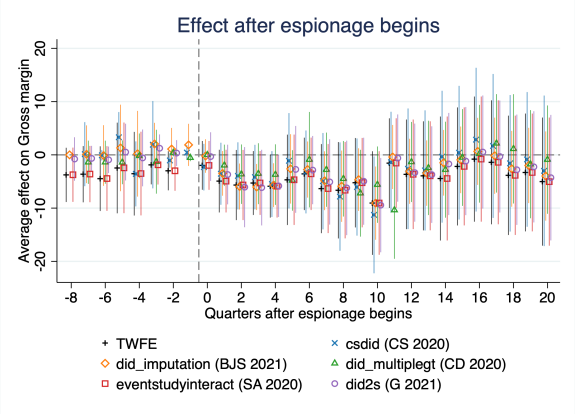
Panel A: log(Assets)



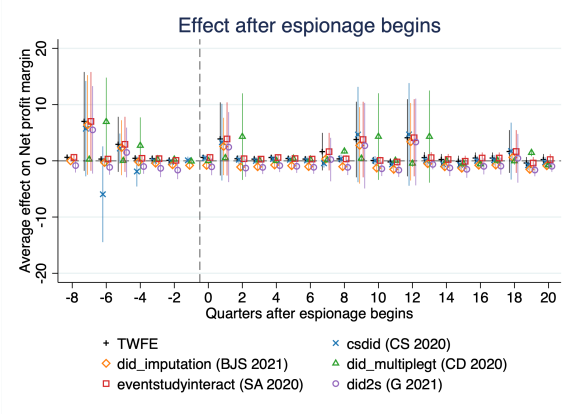
Panel B: log(Intangible assets)



Panel C: Gross margin

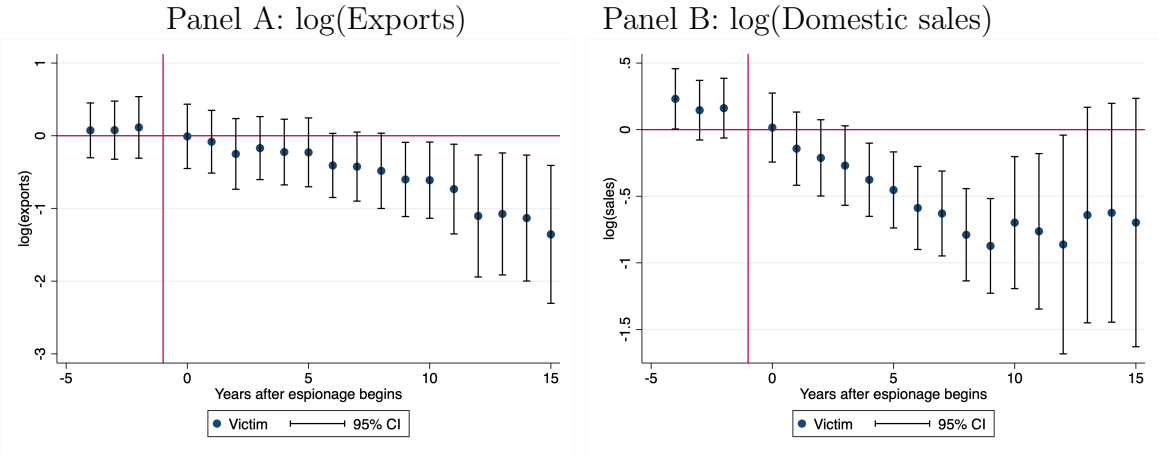


Panel D: Net profit margin



Note: This figure plots coefficients and 95% confidence intervals from various heterogeneous dynamic difference-in-difference specifications. An event is a firm being successfully targeted for economic espionage. The outcome in Panels A is a firm's log(Assets), in Panel B a firm's log(Intangible assets), in Panel C a firm's gross margin, and in Panel D a firm's net profit margin. Black crosses present estimates from a standard two-way fixed effect design, blue crosses present estimates using Callaway and Sant'Anna (2021), orange diamonds present estimates using Borusyak, Jaravel, and Spiess (2023), green triangles present estimates using de Chaisemartrin and D'Haultfoeuille (2024), red squares present estimates using Sun and Abraham (2020), and purple circles present estimates using Gardner (2021). Standard errors are clustered at the firm level.

Figure A.6: Effect of espionage on victim firm log exports and domestic sales

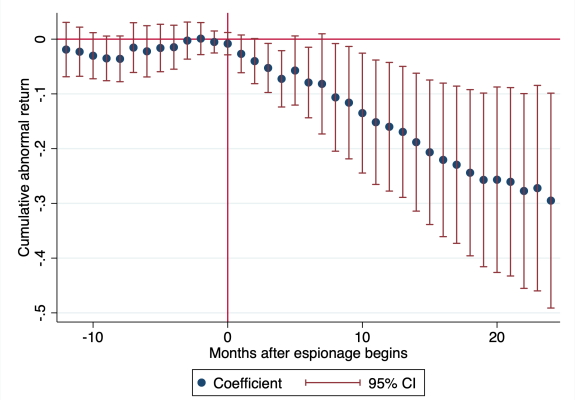


Note: This figure plots coefficients and 95% confidence intervals from a two-way fixed effects event study regression. An event is a firm being successfully targeted for economic espionage. The outcome in Panel A is a firm's log(Exports) and in Panel B a firm's log(Domestic sales). The unit of analysis is a firm by year. Standard errors are clustered at the firm level.

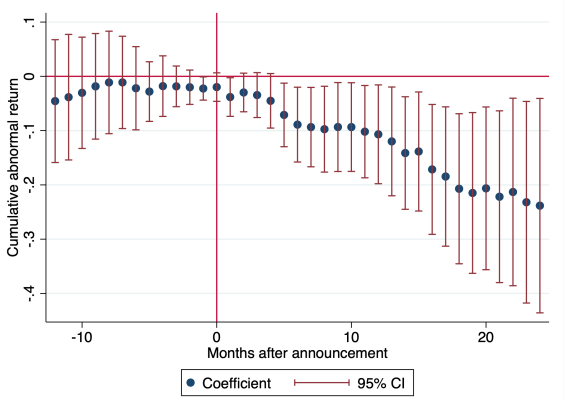
Figure A.7: Effect of espionage on victim firm's cumulative abnormal returns

Panel A: Successful cases

Panel A.1: After espionage begins

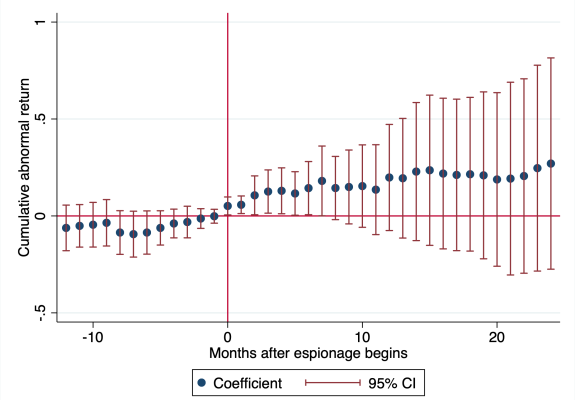


Panel A.2: After publicly announced

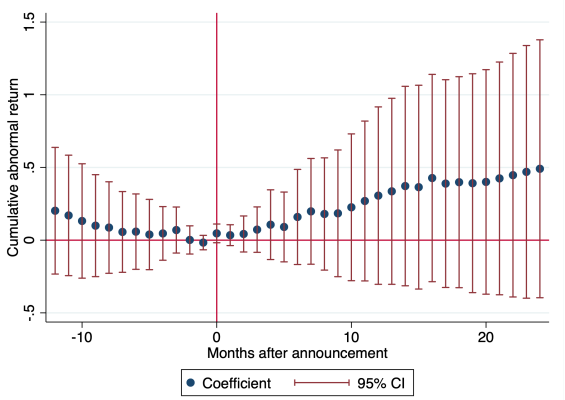


Panel B: Unsuccessful cases

Panel B.1: After espionage begins

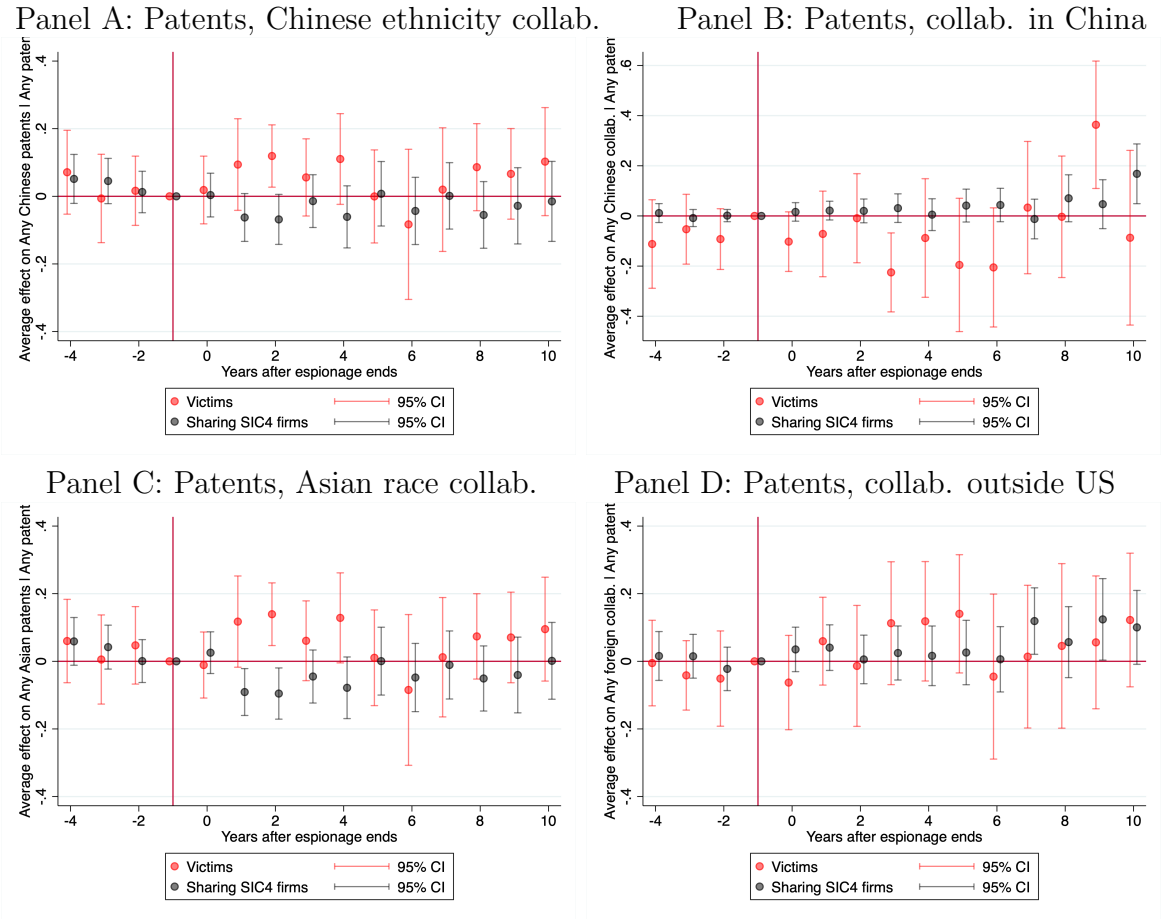


Panel B.2: After publicly announced



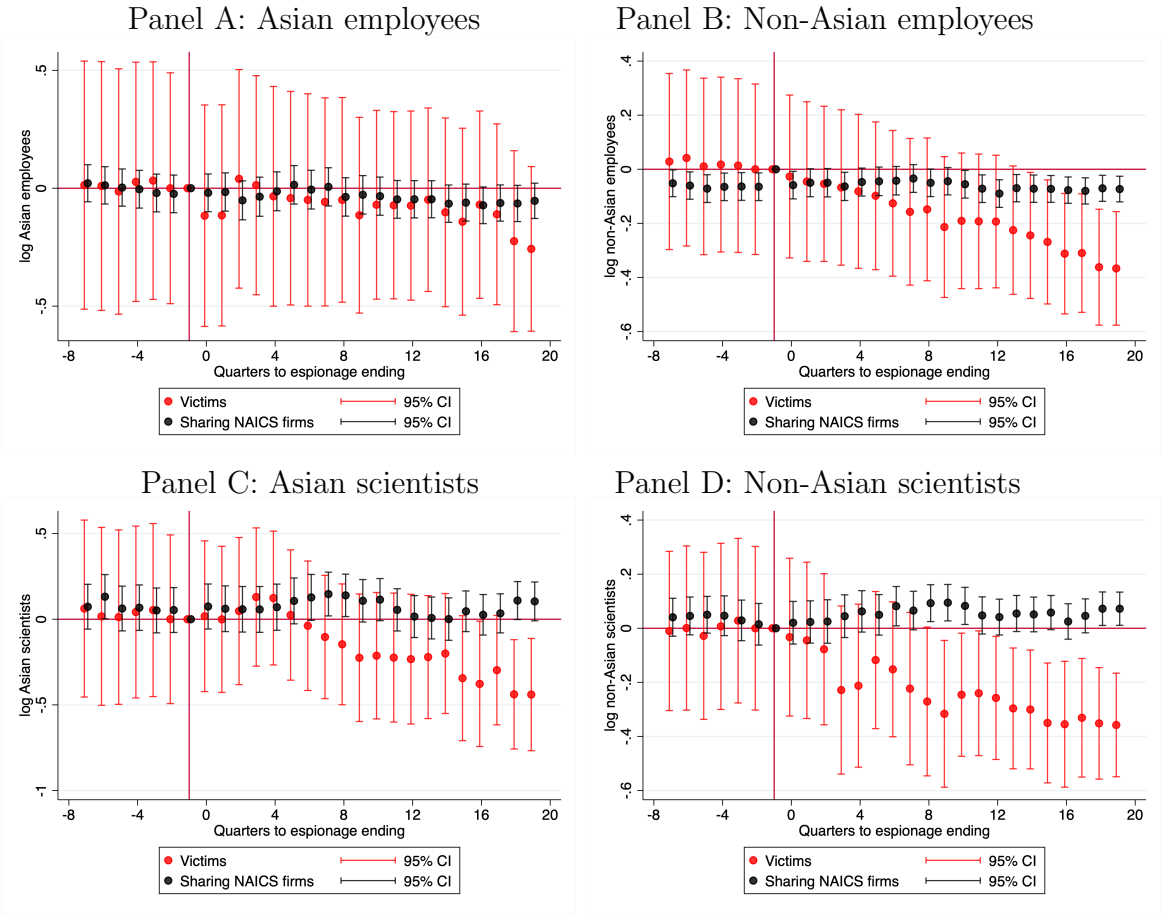
Note: This figure plots coefficients and 95% confidence intervals from regressions on victim firms of economic espionage at various time horizons. In Panel A, an event is a firm being successfully targeted for economic espionage. Panel A.1 uses the timing of when espionage begins (an agent first begins extracting proprietary information) and Panel A.2 uses the timing of when espionage is first publicly announced. In Panel B, events are unsuccessful cases of economic espionage, where the desired information was not successfully given to its intended recipient. Cumulative abnormal stock market returns are computed using Fama-French factors in the period 30 days before espionage begins. Standard errors are robust.

Figure A.8: Effect of espionage on proportion of patents with foreign collaborators, spillovers to industry



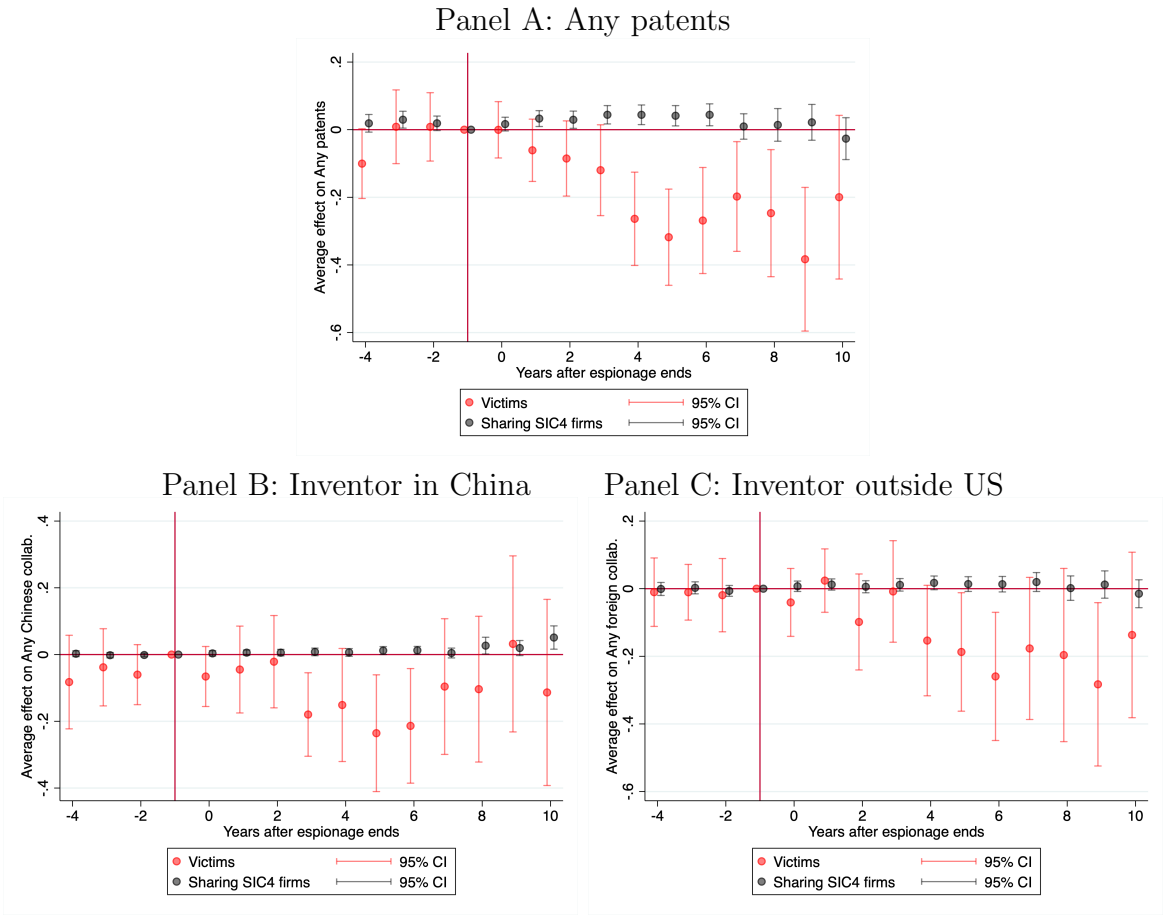
Note: This figure plots coefficients and 95% confidence intervals from a triple differences two-way fixed effects regressions. An event is when an successful economic espionage incident ends. The outcome in Panel A is whether the firm patented with an ethnic Chinese co-author, in Panel B whether the firm patented with a collaborator living in China, in Panel C whether the firm patented with an Asian co-author, and in Panel D whether the firm patented with a collaborator living outside the United States, all conditional on the firm having any patents. The sample consists of all firms in treated industries (SIC-4 codes ever targeted for espionage) and "nearby" never-treated industries (industries sharing an SIC-3 code with treated SIC-4 industries). Coefficients for event-time indicators are plotted in black, while triple difference coefficients for victim firms are plotted in red. Standard errors are clustered at the firm level.

Figure A.9: Effect of espionage on employment by race, spillover to industry



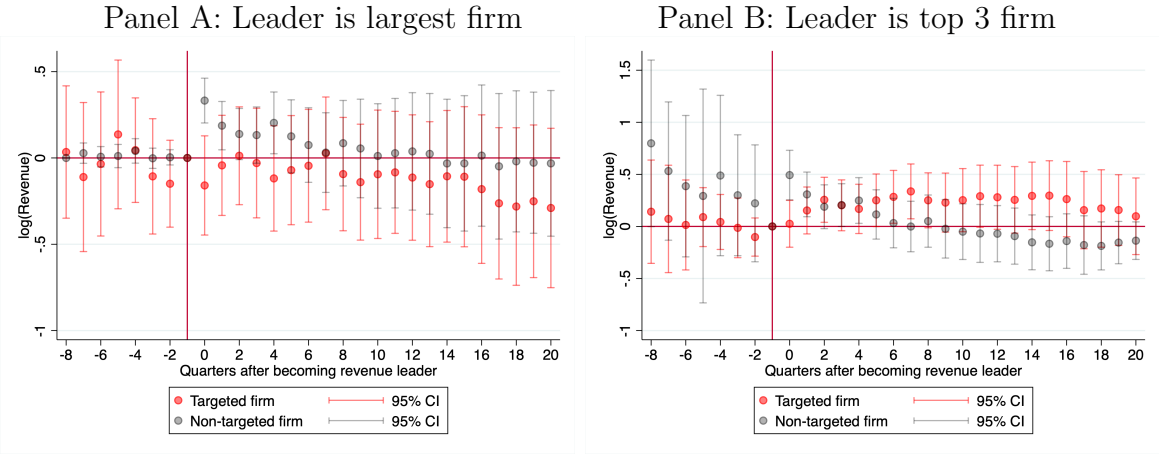
Note: This figure plots coefficients and 95% confidence intervals from a triple differences two-way fixed effects regressions. An event is when an successful economic espionage incident ends. The outcome in each panel is the logged count of the respective employee type. The sample consists of all firms in treated industries (NAICS-6 codes ever targeted for espionage) and all firms in "nearby" never-treated industries (industries sharing an NAICS-4 code with treated NAICS-6 industries). Coefficients for event-time indicators are plotted in black, while triple difference coefficients for victim firms are plotted in red. Standard errors are clustered at the firm level.

Figure A.10: Effect of espionage on patenting, spillover to industry



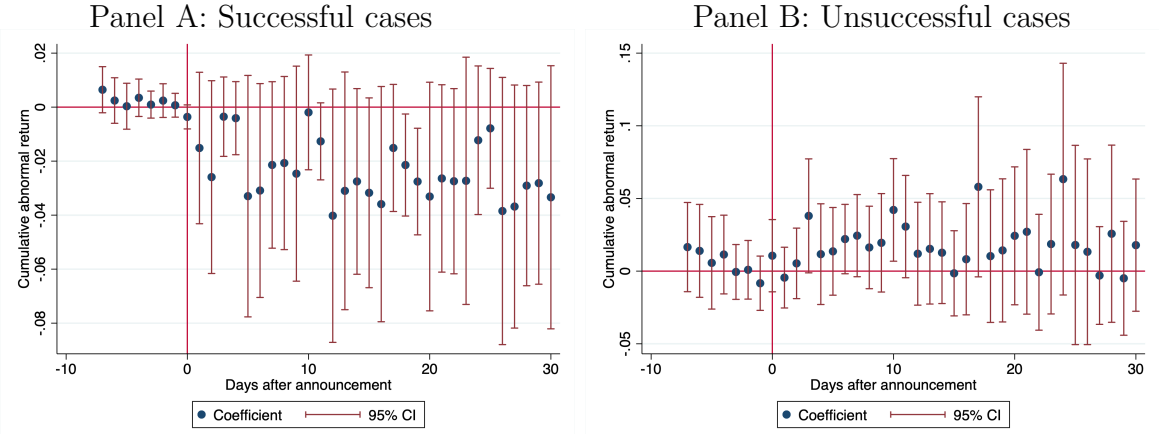
Note: This figure plots coefficients and 95% confidence intervals from a triple differences two-way fixed effects regressions. An event is when an successful economic espionage incident ends. The outcome in Panel A is whether the firm patented in a given year, in Panel B whether the firm patented with an inventor living in China, in Panel C whether the firm patented with an inventor living outside the US. The sample consists of all firms in treated industries (SIC-4 codes ever targeted for espionage) and "nearby" never-treated industries (industries sharing an SIC-3 code with treated SIC-4 industries). Coefficients for event-time indicators are plotted in black, while triple difference coefficients for victim firms are plotted in red. Standard errors are clustered at the firm level.

Figure A.11: Firm log revenue in the quarters preceding and following when they become an industry leader



Note: This figure plots coefficients and 95% confidence intervals from two-way fixed effects event study regressions. An event is a firm becoming a leader in their industry (SIC-4). In Panel A, a leader is defined as the largest firm by revenue. In Panel B, a leader is defined as a top three firm by revenue. The outcome is log(Revenue). Estimates for firms ever targeted for economic espionage are plotted in red, and for non-targeted firms (in targeted industries) in black. Standard errors are clustered at the firm level.

Figure A.12: Effect of espionage announcement on victim firm cumulative abnormal returns, day level



Note: This figure plots coefficients and 95% confidence intervals from regressions on victim firms of economic espionage at various time horizons. In Panel A, an event is the announcement of a firm being successfully targeted for economic espionage. In Panel B, events are unsuccessful cases of economic espionage, where the desired information was not successfully given to its intended recipient. Cumulative abnormal stock market returns are computed using Fama-French factors in the period 30 days before espionage begins. Standard errors are robust.

Table A.1: Industry dynamics by whether an industry has been targeted by espionage

Outcome:	I[Leader at $t-X$ is leader at t]				Dist. (1st - 2nd)	HHI
	Leader = top		Leader = top 3			
	$X=1$	$X=4$	$X=1$	$X=4$		
	(1)	(2)	(3)	(4)	(5)	(6)
Targeted SIC	0.016	-0.011	-0.005	-0.008	-0.302	-0.074
	(0.045)	(0.027)	(0.021)	(0.014)	(0.211)	(0.048)
Constant	0.837***	0.878***	0.905***	0.922***	1.247***	0.409***
	(0.026)	(0.015)	(0.013)	(0.008)	(0.137)	(0.030)
N	98	98	98	98	98	98
Industry size	Yes	Yes	Yes	Yes	Yes	Yes

Notes: This table presents coefficients and standard errors for regressions at the SIC level. The sample is restricted to SIC codes where an industry sharing an SIC 3 code was ever targeted for economic espionage. The independent variable of interest is whether an industry has been targeted by espionage. The outcome in columns 1-4 is the average probability of whether a leader in a given quarter $t-X$ is still a leader in quarter t. In columns 1 and 2, leader is defined as being the largest firm by revenue in industry, while in columns 3 and 4, leader is defined as being a top 3 firm by revenue. In columns 1 and 3, $X=1$, while in columns 2 and 4, $X=4$. The outcome in column 5 is the distance in log revenue between the largest and second largest firm. The outcome in column 6 is the average HHI within the industry. Industry size controls include (average) number of firms in industry, quarters of data available, and average log revenue. * significant at 10% ** significant at 5% *** significant at 1%.