Economic Espionage and Innovation Restrictions*

Andrew Kao† Karthik Tadepalli‡

December 31, 2025

Abstract

We provide systematic evidence on the economic damages from espionage to US firms and industries. Compiling a comprehensive dataset of publicly disclosed espionage incidents from 1995-2024, we establish that espionage has substantial negative effects on targeted firms. In an event-study design, revenues and R&D expenditures at targeted firms decline by roughly 40% within five years, with effects persisting for up to a decade. These effects do not appear for firms unsuccessfully targeted for espionage, supporting a causal interpretation. These firm-level damages translate into measurable aggregate effects on US industry: exports in targeted sectors decline by 60% over a decade. Given these substantial damages, we investigate whether firms restrict knowledge sharing in response to espionage. Across a wide range of outcomes, we find no evidence of such restrictions. Firms do not reduce their patenting with foreign inventors, and do not discriminate in employment based on perceived espionage risk. Overall, espionage has clear economic harms to targeted firms and US industry, but firms are puzzlingly unresponsive in how they manage innovation.

*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

Economic espionage represents a substantial threat to US firms and industries. As China has grown economically, it has pursued various strategies to acquire knowledge and technology from US firms, with economic espionage being one of the most direct methods. From high-profile cyber intrusions targeting semiconductor companies to insider theft at pharmaceutical firms, espionage incidents have become increasingly common. The US government has responded with heightened enforcement through the Economic Espionage Act and the China Initiative, reflecting concerns about the economic damages from these incidents (Miller, 2022; Hvistendahl, 2021). Despite this policy attention, systematic empirical evidence on the economic consequences of espionage remains limited. This makes it important to understand: what are the economic harms from espionage to targeted firms and US industry, and how do firms respond to being targeted?

To answer these questions, we compile a comprehensive dataset on publicly disclosed 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. We link this case-level data to firms, which 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 40% after 5 years, with effects persisting for 10 years. These results are robust to alternative identification strategies, and they hold for a variety of other firm outcomes including total assets and intangible assets. Importantly, we find no effect on any of these outcomes when espionage attempts are unsuccessful (i.e. when no knowledge was transferred). This placebo test provides strong evidence that our estimated effects are not driven by violations of the parallel trends assumption, but rather reflect the causal impact of successful espionage on firm revenues and R&D.

To probe the mechanisms behind these effects, we examine heterogeneity across different types of incidents. We find that the revenue losses from espionage are concentrated in cases where firms claim high economic losses, and in industries where industry-wide R&D spending is relatively low. The first result suggests that espionage is most harmful when it targets key technologies that are difficult to replace. The second result suggests that espionage is most harmful in industries where the key technologies are established (and thus spending on developing new technology is low). Together,

these heterogeneity analyses paint a picture whereby espionage makes a firm's valuable technology obsolete.

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 American exports in targeted sectors decline by 60%. Surprisingly, we find that Chinese exports do not rise in response to espionage; they decline in the short term before recovering in the long term, with no net gain. Global exports in targeted sectors decline by 10%, suggesting that the harms to the US are not offset by benefits to China. These results demonstrate that the economic damages from espionage extend beyond individual firms to have measurable aggregate effects on US industry, and are not simply a redistribution of market share from one firm to another within the United States. Moreover, they suggest that Chinese firms are not able to capture the full advantage created by espionage.

Having established the substantial economic harms from espionage, we turn to a natural follow-up question: how do targeted firms respond to espionage? In particular, given concerns that geopolitical tensions could lead to restrictions on knowledge diffusion that harm innovation and growth, we test whether firms reduce their knowledge sharing in response to being targeted. We study these potential innovation restrictions across two margins: knowledge-sharing through patenting, and employment decisions that could screen out employees perceived as "high espionage risk." We estimate the first margin by linking firms to patents, and the second margin through matched employer-employee data from LinkedIn.

Across a wide range of outcomes, we find no evidence that firms reduce knowledge sharing in response to espionage. Espionage does not affect the patent-to-R&D ratio, the probability that a firm patents with an inventor in China or outside the US more broadly, or how many times the firm's patents are cited. We also find no evidence that firms discriminate in their employment decisions based on perceived espionage risk. While the number of Asian scientists at targeted firms declines by more than the number of non-Asian scientists, we do not find evidence that this differential decline is caused by discrimination. Specifically, we find no decline in diversity and inclusion scores at targeted firms, suggesting that the employment patterns may reflect worker decisions rather than firm-side discrimination.

Together, our results establish that economic espionage causes substantial economic

harm to both targeted firms and US industry more broadly, but find no evidence that firms respond by restricting knowledge flows in ways that could further harm innovation. In short, we document clear economic damages from espionage, but do not find that firms change their management of innovation and knowledge sharing in response.

Related Literature This paper relates to four strands of the literature. First, we contribute to research on the value of trade secrets. Our paper is closely connected to two recent papers studying the effects of trade secret theft and espionage on firms. Curti et al. (2024) examine how corporate innovation responds to the theft of trade secrets, while Michaelides et al. (2024) study the value of trade secrets as imputed from espionage incidents. Relative to these papers, we make three contributions. First, each paper's analysis focuses on a single outcome in targeted firms (innovation and market capitalization, respectively), while we examine a much broader set of firm outcomes including revenue, R&D, assets, patenting behavior and employment discrimination. Second, our analysis of unsuccessful attempts at espionage provides a stronger argument for causality. Third, we analyze the industry-level effects of espionage using international trade data, allowing us to characterize the net effects of espionage on US industry and show that the damages extend beyond redistribution between firms within the US. Fourth, our dataset of espionage incidents is more comprehensive in scope than the datasets of these two papers (covering 164 incidents, compared to 52 incidents and 72 incidents respectively in these two papers). This makes our analysis more generalizable, despite the difficulty of observing espionage empirically.

Second, we contribute to research on geopolitical tensions and international economic relationships. The growing literature on geopolitical tensions has primarily focused on trade and investment relationships between countries (Clayton, Maggiori, and Schreger, 2023), with knowledge and technology relationships being more difficult to study. Some papers within this framework study 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 provide systematic evidence on how economic espionage affects firms and industries today, and to test whether it induces restrictions on innovation that could have broader economic consequences.

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. A central question in these models is how competition affects innovation incentives, with theory predicting ambiguous effects: competition can spur innovation by increasing the returns to escaping competition (the "escape competition" effect), but can also reduce innovation by decreasing the rents available to innovators (the "Schumpeterian" effect). Building on these models, 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. Economic espionage represents an exogenous shock to the competitive pressure faced by industry leaders, as it allows competitor firms (particularly Chinese firms) to acquire the technologies that gave leaders their competitive advantage. Our finding that espionage reduces R&D spending by targeted firms provides evidence that increased competition reduces innovation, consistent with the Schumpeterian channel dominating in our setting.

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 and its economic effects on firms and industries. We also contribute by testing whether counter-espionage concerns lead to discrimination in employment, finding that firms do not appear to become more discriminatory after espionage incidents.

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 economic damages from espionage on targeted firms and industries. Section 5 analyzes whether firms respond to espionage with innovation restrictions. 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 recognized as a tool of statecraft. In the 19th century, the US chemical industry grew to the technological frontier through hiring German chemists who brought trade secrets (Hounshell, 1988). 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, economic espionage is believed to be widespread. For example, in a report uncovering a series of coordinated breaches of over fifty global companies, 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 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 is 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 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 emblematic case comes from Orbit Irrigation, an American 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 or market research that can also be important to businesses.

Another example is the case of Valspar Corp, an American paint company. David Lee—a technical director at Valspar at the time—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.

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 documented instances of foreign economic espionage against US firms since 1990. For the purposes of this study, we define economic espionage as theft of a firm's 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 include cases of explicit forced 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.[1]

[1]The prior literature studying the effect of such breaches (Gatzlaff and McCullough, 2010; Arcuri, Brogi, Gandolfi, et al., 2018) finds small, negative effects on targeted firms.

Sample Construction To build a comprehensive database of incidents of economic espionage against the United States, we make use of the following sources:

1. First, we query 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.[2]

2. Second, we search through all Department of Justice press releases about economic espionage indictments,[3] alongside relevant publications such as the DOJ's Pro IP Act Annual Reports.[4]

3. Third, we complement these primary sources with compilations of espionage cases created by other third parties. These come from a wide range of actors, specifically 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. Finally, we conduct our own search of news articles, corporate press releases, and cybersecurity firm announcements.[5]

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

[2]We search for references to the relevant legal statute, 18 U.S.C. § 1831 and 1832, as well as "economic espionage." In three instances, we found a sealed search warrant and were unable to recover any further details regarding the incident.

[3]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.

[4]This use of DOJ press releases combined with the CourtListener data supersets the data used by Fang and Li (2021) and Michaelides et al. (2024) to study Economic Espionage Act cases.

[5]In particular, we search for news relating to "economic espionage" on Google News in one year time windows from 1990 to the present, we search the universe of US equity earnings call transcripts for "economic espionage", and the websites of all cybersecurity firms mentioned or involved in the cases above (e.g., McAfee, Symantec, Mandiant, Crowdstrike, Kaspersky, etc).

was a cybersecurity incident or not, alongside the victim companies targeted, and the suspect firm (when available).[6]

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. The most targeted industry is semiconductors. Frequently targeted industries, including plastics, pharmaceuticals, and aircraft manufacturing, tend to be knowledge-heavy in nature, as well as reliant on trade secrets to protect their competitive advantage. They are also more likely to have military significance; in Figure 2 we plot the share of industries that are "dual-use" (Kang, 2024) by whether they are targeted by espionage or not. We find that 88% of SIC codes targeted in our data are dual-use, compared to 47% of SIC codes in general. Thus, targeted SIC codes are twice as likely to be dual-use as the average SIC code, consistent with strategic motivations for espionage.

More than three-quarters of our incidents take place in a repeatedly targeted industry. In Figure 3, 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 (public) 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.[7] This suggests that the targeting of firms occurs

[6]This information was not always trivial to collect. 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.

[7]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.

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", and we use it as our industry definition in our analysis.

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. 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. As a result, even though the effect of espionage on suspect firms is an important question, our data is too noisy to answer it. Thus, our analysis of 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, which may still remain undetected, 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. For our research question, economic espionage incidents are best understood as a window into how firms react and change their openness to knowledge diffusion in response to economic espionage information shocks. 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 unknown cases.[8]

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

3.2 Firm-Level Data

Out of 164 cases of economic espionage, we are able to identify a victim firm in 130 incidents. 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 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 an annual 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 estimate 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."[9] 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

[9]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.

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").[10] 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 (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 had no effects on firm revenues, we might 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.

[10] Details of this construction are in Appendix A.1.

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.

4.1 Baseline Specification

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:

$$y_{i,t} = \sum_{k=-4}^{10} \gamma_k D_{i,t+k} + \alpha_i + \alpha_{j(i),t} + \varepsilon_{i,t} \tag{1}$$

where i denotes a firm, t a year, 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 year $t + k$. 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 year fixed effects are actually industry-year fixed effects. In other words, we are comparing targeted firms to untargeted firms *within the same industry*. This feature is important because industries 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 knowl-

edge/technology. However, the *welfare* effects of espionage are likely to be dominated by how it affects firm innovative activity.[11] As a result, we use R&D expenditures to capture this dimension of the effects of espionage.

Figure 4, 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 40-50% within 5 years of espionage beginning, with effects continuing to persist for up to 10 years. 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 innovative capacity. We find no evidence of pre-trends in the event study.

4.2 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

[11] See, for instance, Myers and Lanahan, 2022; Jones and Summers, 2020; Arque-Castells and Spulber, 2022.

parallel trends. Conversely, a null effect in this placebo sample provides evidence for the parallel trends assumption—stronger support than is normally available to difference-in-difference research designs.

In Figure 4 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.

To verify that this null effect in the placebo test is not simply noise, we estimate a triple-difference specification in Table 2 that allows us to specifically test whether the treatment effect differs between the two groups (successful firms and unsuccessful firms). We find that even with the small size of our placebo sample, we can reject that the placebo effect on revenue is the same as the effect on successful firms—providing evidence that our effects are not simply driven by pre-trends. However, R&D is a noisier outcome, and the effect we show in Figure 4 only becomes large many years after the espionage. This is why the triple difference coefficient, which includes the years just after espionage, is smaller and thus can't be separated from the placebo.

4.3 Mechanisms

To understand the mechanism by which espionage affects firms, we estimate heterogeneous effects of espionage on firms and plot the results in Figure 5

First, we separate cases based on whether the damages claimed by the victim firm are above or below the median claimed damages, and estimate Equation 1 separately for these two groups. Panels A.1 and A.2 show that our estimated revenue effects are concentrated entirely in cases with above-median claimed damages. Claimed damages are a legal construct that firms calculate based on the self-assessed market view of their stolen technology. Thus, cases with high claimed damages are cases where the stolen technology was especially critical to the firm's competitive edge, and espionage may represent the loss of this competitive edge.[12]

Second, we separate cases based on whether the targeted industry's baseline R&D spending is above or below the median for targeted industries. Panel B.1 shows that the revenue damages from espionage are most pronounced in industries with below-median R&D spending. Although potentially counterintuitive, our preferred interpretation is

[12]We also interpret this result as evidence supporting a causal interpretation—if our estimates were driven by differential trends or other threats to causal inference, we would not expect the negative effects to be concentrated among firms that claimed high damages.

that espionage is most damaging when a firm is in an industry with relatively few key technologies, compared to in a more fast-moving sector where technologies become obsolete quickly and/or the marginal value of each technology is lower.

Third, we separate cases based on how concentrated the targeted industry is (as measured by HHI). Panel C.1 shows that the revenue effects of espionage are common for both low-HHI and high-HHI industries, but Panel C.2 shows that espionage reduces R&D only in low-HHI industries. This heterogeneity suggests that in more competitive industries, falling revenue necessitates reduced R&D spending—but in concentrated industries, targeted firms (who are usually the industry leaders, as shown by Figure 3) still have enough rents to sustain R&D spending.

Together, these heterogeneity analyses paint a picture whereby espionage makes a firm's valuable technology obsolete. Thus, espionage is less harmful when these technologies are less valuable or when the industry's high rate of R&D spending means the natural obsolescence rate of technology is higher.

4.4 Robustness Checks and Additional Analyses

We briefly report additional robustness checks, which are described in more detail in Appendix B. First, 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.2). Second, in addition to firm revenue and R&D expenditures, we show that espionage also reduces a firm's total assets and intangible assets by a similar amount (Figure A.3), and that both domestic sales and exports decline (Figure A.5). Third, we relax the assumption that firms in the targeted industry are untreated, allowing for spillovers to those firms (Figure A.4). Fourth, we look at how firms' stock returns are affected by both the onset and announcement of espionage, finding that both events lead to persistent declines in returns, consistent with losses from both real factors and the market's perception of these incidents (Figure A.6). Finally, we show that results are unlikely to be driven by mean-reversion of leader firms (Figure A.7) or by selection of targeted industries (Table A.1).

4.5 Effects on an Aggregate: Exports

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, especially if the reallocation happened within a country.

To understand these aggregate effects, we test how espionage incidents affect exports in both the US and China. We use trade data to capture industry-level effects for three reasons. First, it covers all firms operating in each country, including non-publicly listed firms that would not appear in Compustat. Second, in Ricardian models of trade, 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 cleanest 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—those that 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.[13] 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 the 129 where the suspect country is China.

We plot results in Panel A of Figure 6. We find that ten years after espionage

[13]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. The US and China interaction coefficients are robust to the inclusion of HS6-year fixed effects.

occurs in a sector, exports by the US fall by 60%. Puzzlingly, exports from China also fall in the short term before recovering in the long term. These results suggest that the US is harmed by economic espionage and that China does not benefit in a way that compensates for these loses.

These effects are surprisingly large. Are they due to selection of which industries are targeted for espionage? 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 6 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 6 are truly causal. However, we do see Chinese exports rising in sectors even when espionage is unsuccessful. Thus, it is 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.

We note two additional reasons that effects may be large. First, many targeted firms are large, multiproduct firms, and so losses in affected HS6 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. Given the size distribution of firms follows a power law (Axtell, 2001) and that many sectors are repeatedly targeted, this can reconcile the large estimated effects on exports.

5 Knowledge Diffusion Under Espionage

The previous section has established the direct effect of espionage on firm and industry outcomes. 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.

5.1 Patent-Based Openness

One way to understand firm openness and knowledge-sharing with the world is through patenting behavior. Patenting inherently involves disclosure of inventions, providing knowledge spillovers to the rest of the world. Patenting data additionally includes

information about how the technology was produced (e.g., the location of collaborators) that indicate how internally open the firm is. Thus, we can get a richer understanding of how espionage affects knowledge diffusion by measuring patenting outcomes.

We estimate Equation 1 with patent-based outcome measures, with two modifications. 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.[14]

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. We address this concern by directly testing it. In Section 5.3, we show that untargeted firms do not 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 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 is 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 openness. We proxy for this measure of "secrecy" by measuring patents filed per dollar of R&D expenditure—reflecting the fact that if the

[14]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.

results of R&D were instead held as trade secrets, that would decrease the patents filed per R&D dollar. In Figure 7, 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.[15]

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 Employment Responses

The key vector for espionage is employees of the targeted firm. Thus, an important margin of response for targeted firms is how they adjust their employment decisions. In particular, we ask: 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. On the other hand, employees themselves may also endogenously respond to espionage—employees, seeing the writing on the wall, may also leave the firm for greener pastures.

[15] One possible interpretation of the increase in patenting per R&D dollar spent is that as R&D spending declines, the firm cuts R&D lines with lower probability of success, leading to a higher patent output per R&D dollar.

We test both the "discrimination hypothesis" and the "outside option hypothesis" using LinkedIn data provided by Revelio Labs, with additional features estimated by Revelio from the raw LinkedIn data. Our first analysis focuses on the employment of ethnically Asian scientists. Revelio classifies employees into ethnic categories based on their name, allowing us to observe the number of ethnically Asian employees at each firm over time.[16] Revelio classifies job titles into 1500 employment categories, which we manually classify as "scientist" and "non-scientist" jobs to determine whether a job involves R&D work (e.g. "process development engineer", "research scientist"). With these two categorizations, we can 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. Figure 8, 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 equality shows that these coefficients are marginally statistically different (p=0.068).

This pattern is consistent both with discrimination against ethnically Asian scientists and with ethnically Asian scientists having better outside options that lead them to leave the firm at higher rates. To distinguish between these two explanations, we estimate the effect of espionage on diversity and inclusion within targeted companies. Revelio captures the text of employee reviews of each firm, from which we construct DEI scores that measure how positively employees speak about the inclusivity of their work environment. Details on how this data is constructed can be found in Appendix A.2. If being targeted for espionage led firms to discriminate against Asian scientists, we might expect to see lower DEI scores based on reviews from scientists, especially compared to non-scientists for whom we do not see this differential selection pattern.

Figure A.9 shows that after espionage, there is no decline in the DEI scores given by scientists (or by non-scientists). Thus, we conclude that the differential decline in the employment of Asian scientists is likely due to those scientists having stronger outside options (and/or greater anticipation of firm difficulties), rather than due to discrimination.

[16]This is of course not a perfect proxy for the perceived 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.

Taken together, these findings suggest a surprising lack of response by firms 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. Nor do they attempt to screen out ethnically Asian scientists due to perceived espionage risk.

Given the large estimated damages from espionage, we initially hypothesized that firms would respond to Chinese espionage by adopting security measures that screened out Chinese employees. However, that does not seem to be the case. One explanation could be because firms recognize the value of knowledge flows and allocating scientific talent correctly, and believe that reducing patenting with Chinese inventors or screening Chinese scientists would be even more damaging to them than any risk of espionage.

5.3 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 only an independently important margin of response, but also an identification threat to the previous sections—by taking non-targeted firms as never-treated, we risk underestimating the endogenous response to espionage that could be common across firms.

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, 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. Then the etsimating equation is

$$y_{i,t} = \sum_{k=-4}^{10} \gamma_k D_{i,t+k} + \sum_{k=-4}^{10} \gamma_k D_{j(i),t+k} + \alpha_i + \alpha_t + \varepsilon_{i,t} \tag{4}$$

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. We only keep the first incident targeting an industry in estimation.

In Figure A.11, 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.[17] 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 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.[18]

[17] 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.

[18] One potential limitation is that 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

6 Conclusion

This paper provides systematic evidence on the economic damages from espionage to US firms and industries. We show that economic espionage has substantial negative effects on targeted firms, with revenues and R&D expenditures declining by roughly 40% within five years, with effects persisting for up to a decade. These damages are concentrated in cases where firms claim high economic losses and in industries with lower R&D intensity, suggesting that espionage is most harmful when it targets key technologies that are difficult to replace. Importantly, we find no effects when espionage attempts are unsuccessful, providing strong evidence for a causal interpretation of our results.

These firm-level effects translate into measurable aggregate effects on US industry. American exports in targeted sectors decline by roughly 60% over a decade. Surprisingly, Chinese exports in these sectors do not rise in response to espionage, suggesting that the damages to the US are not offset by gains to China, with global exports in targeted sectors declining by 10%. These results demonstrate that the economic consequences of espionage extend well beyond the individual firms targeted, and are not simply a redistribution of market share among US firms.

Given these substantial economic damages, a natural question is whether firms respond by restricting their knowledge sharing in ways that could further harm innovation and growth. Across a wide range of outcomes, we find no evidence of such responses. Targeted firms do not reduce their patent-to-R&D ratio, do not become less likely to patent with inventors in China or outside the US, and do not see reduced citations to their patents. We also find no evidence of discrimination in employment decisions. While the number of Asian scientists at targeted firms declines differentially compared to non-Asian scientists, this pattern appears to be driven by Asian scientists having better outside options rather than by firm-side discrimination, as evidenced by the lack of decline in diversity and inclusion scores at targeted firms.

These findings have important implications. First, from a policy perspective, our results establish that economic espionage causes substantial economic harm to US firms and industries, validating policy concerns about espionage. The aggregate effects on exports demonstrate that these damages affect broader US competitiveness in targeted sectors, as well as negative spillover effects abroad. Second, our results provide evidence on the effects of competition on innovation. Economic espionage represents

rule out with our data.

an exogenous shock to competitive pressure faced by industry leaders, and our finding that it reduces R&D spending provides support for the Schumpeterian channel whereby increased competition reduces innovation incentives.

Third, despite these substantial damages, we find no evidence that firms respond by restricting knowledge sharing in ways that could create additional harm to innovation and growth. This suggests that concerns about geopolitical tensions leading to widespread restrictions on knowledge diffusion may be overstated, at least in the private sector response to espionage incidents. The fact that firms do not reduce patenting or international collaboration in response to espionage is particularly notable given the magnitude of the damages we document.

Several important questions remain for future research. First, our results raise the question of why firms do not appear to restrict knowledge sharing in response to espionage despite the substantial damages they experience. One possibility is that firms recognize that the benefits of open innovation and international collaboration outweigh the espionage risks. Another possibility is that the knowledge embodied in patents poses relatively little espionage risk compared to other forms of proprietary information, raising broader questions about the role of patents in knowledge disclosure.

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. We cannot make claims about the welfare effects of espionage using the heavily selected sample we observe. Future research could use confidential data from security firms or governments to gain a more representative picture of economic espionage events, and thus be able to make more confident claims about the typical espionage case than we can in our setting.

Third, 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 knowledge production in both countries.

Finally, a caveat is in order for interpreting our results. In examining the economic impacts of espionage, we are aware of the political and racial undertones of discussions about Chinese economic espionage. It is important to highlight that most corporate

espionage cases do not involve a foreign country at all, but instead come from domestic competitors (Fang and Li, 2021). In our dataset and analysis, we focus on foreign economic espionage and Chinese economic espionage in particular, because Chinese economic espionage is an active policy issue of large importance. But 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. Our findings should not be taken as a justification to lower the standards of evidence for alleging economic espionage in particular cases.

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] Maria Cristina Arcuri, Marina Brogi, Gino Gandolfi, et al. "The effect of cyber-attacks on stock returns". In: *Corporate Ownership & Control* 15.2 (2018), pp. 70–83.

[4] Pere Arque-Castells and Daniel F Spulber. "Measuring the private and social returns to R&D: Unintended spillovers versus technology markets". In: *Journal of Political Economy* 130.7 (2022), pp. 1860–1918.

[5] Robert L Axtell. "US firm sizes are zipf distributed". In: *Science* 93 (2001), pp. 1818–1820.

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

[7] Filippo Curti et al. "Corporate Espionage and Innovation: Evidence from the Theft of Trade Secrets". In: *Available at SSRN* (2024).

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] Kevin M Gatzlaff and Kathleen A McCullough. "The effect of data breaches on shareholder wealth". In: *Risk Management and Insurance Review* 13.1 (2010), pp. 61–83.

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

[15] 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/.

[16] 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.

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

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

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

[20] Benjamin F Jones and Lawrence H Summers. *A calculation of the social returns to innovation*. Vol. 27863. National Bureau of Economic Research, 2020.

[21] Minsoo Kang. "Export Controls on Dual-Use Items and the Shifting Landscape of Trade and Innovation". In: (2024). Working paper.

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

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

[24] Alexander Michaelides et al. "The Value of Trade Secrets: Evidence from Economic Espionage". In: *Available at SSRN 4866808* (2024).

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

[26] Kyle R Myers and Lauren Lanahan. "Estimating spillovers from publicly funded R&D: Evidence from the US Department of Energy". In: *American Economic Review* 112.7 (2022), pp. 2393–2423.

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

[28] 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.

[29] 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.

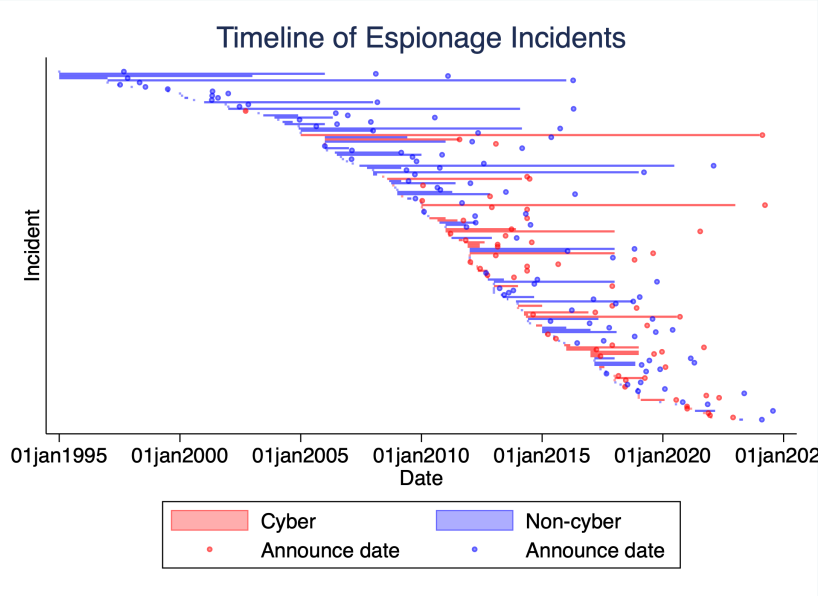
[30] New York Times. "Air France Denies Spying on Travelers". In: *The New York Times* (Sept. 1991). Accessed on Jan 6, 2025. URL: https://web.archive.org/web/20151016000311/http://www.nytimes.com/1991/09/14/news/14iht-spy_.html?pagewanted=1.

[31] 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.

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

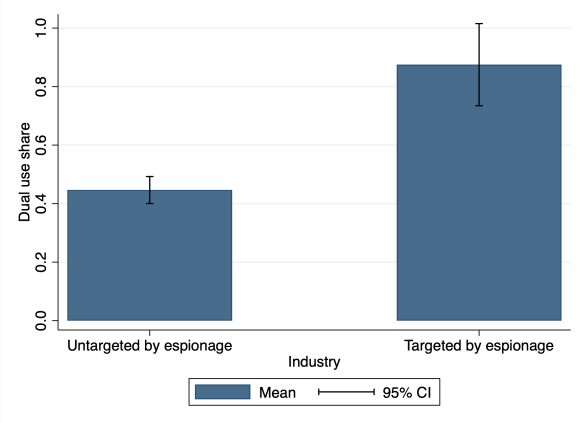
Figures and Tables

Figure 1: Timeline of espionage incidents



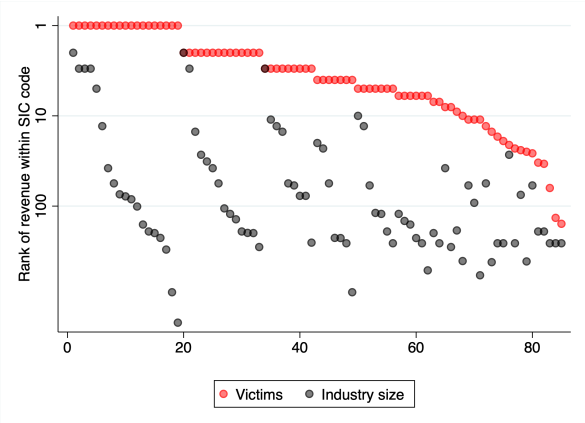
Note: This figure presents a timeline of economic espionage incidents against firms in the United States since 1995. Each row contains a separate incident. The shaded bars span the duration in which espionage occurs (the beginning of the bar corresponds to when espionage began, and the ends of the bar 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: Share of industries that are dual-use by whether targeted for espionage



Note: This figure presents sample means and 95% confidence intervals of the share of industries that are dual-use, split by whether they are targeted or untargeted by espionage. Industries are classified as dual-use or not based on Kang, 2024.

Figure 3: Rank of victim firms by revenue in industry

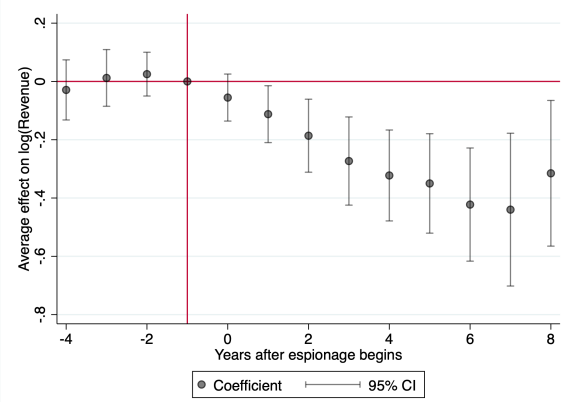


Note: This figure plots the rank of victim firm revenue within their industry (SIC code) in red, and the size of their industry in gray. Firms are ordered by rank, and then industry size. The y-axis uses a log-scale. Revenue is calculated as the average value prior to an espionage incident taking place.

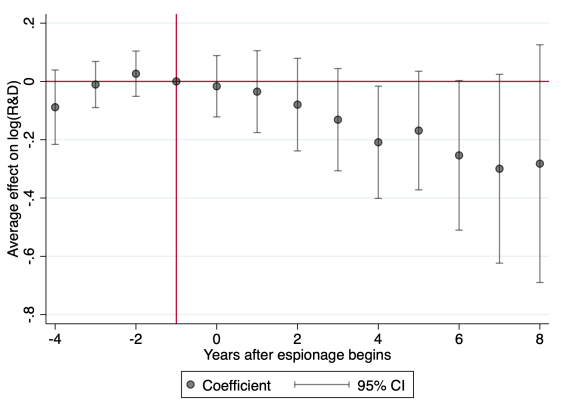
Figure 4: Effect of espionage on victim firm's log revenue and R&D expenditures

Panel A: Successful cases

Panel A.1: log(Revenue)

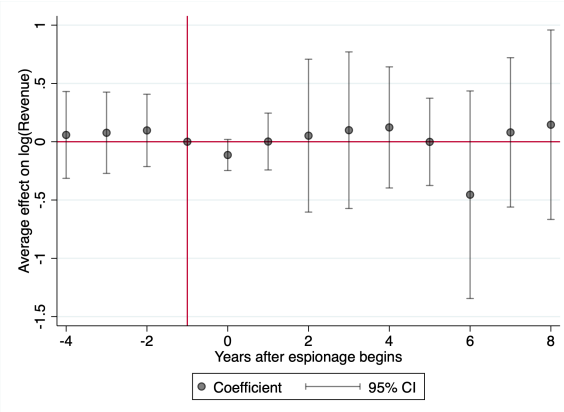


Panel A.2: log(R&D)

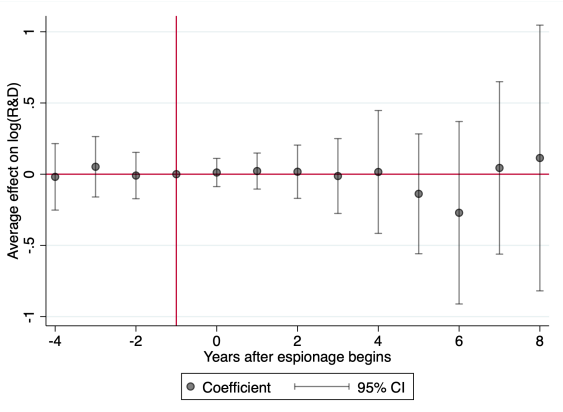


Panel B: Unsuccessful cases

Panel B.1: log(Revenue)



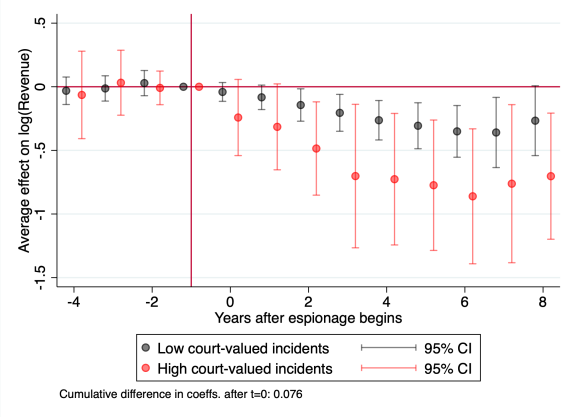
Panel B.2: log(R&D)



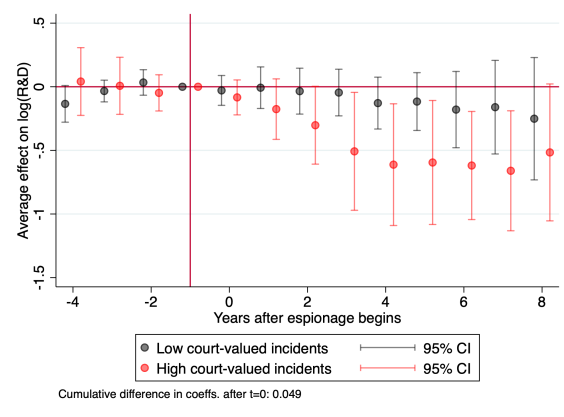
Note: This figure plots coefficients and 95% confidence intervals from a two-way fixed effects event study regression. In Panel A, an event is a firm being successfully targeted for economic espionage. In Panel B, events are unsuccessful cases of economic espionage, where the desired information was 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 5: Heterogeneous effects of espionage

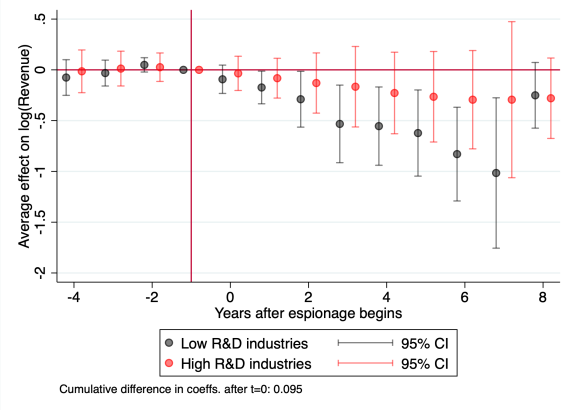
Panel A.1: By value, revenue



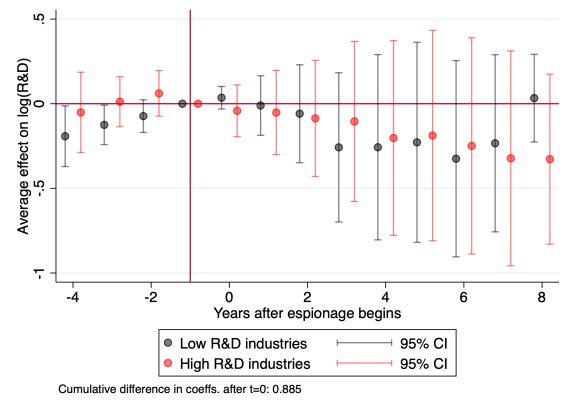
Panel A.2: By value, R&D



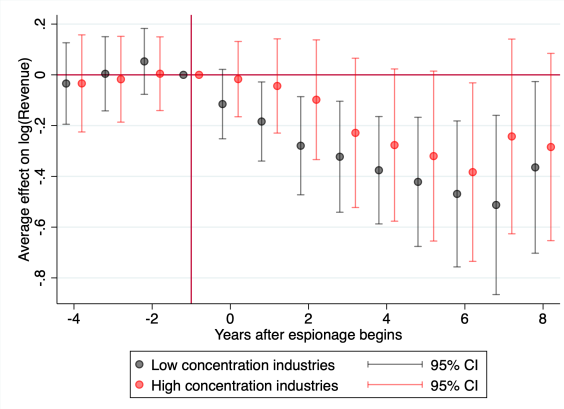
Panel B.1: By industry R&D, revenue



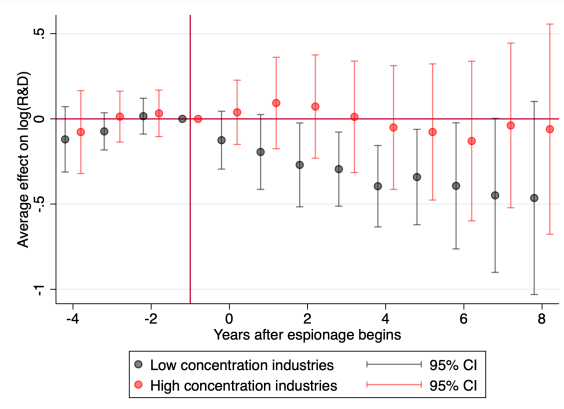
Panel B.2: By industry R&D, R&D



Panel C.1: By HHI, revenue

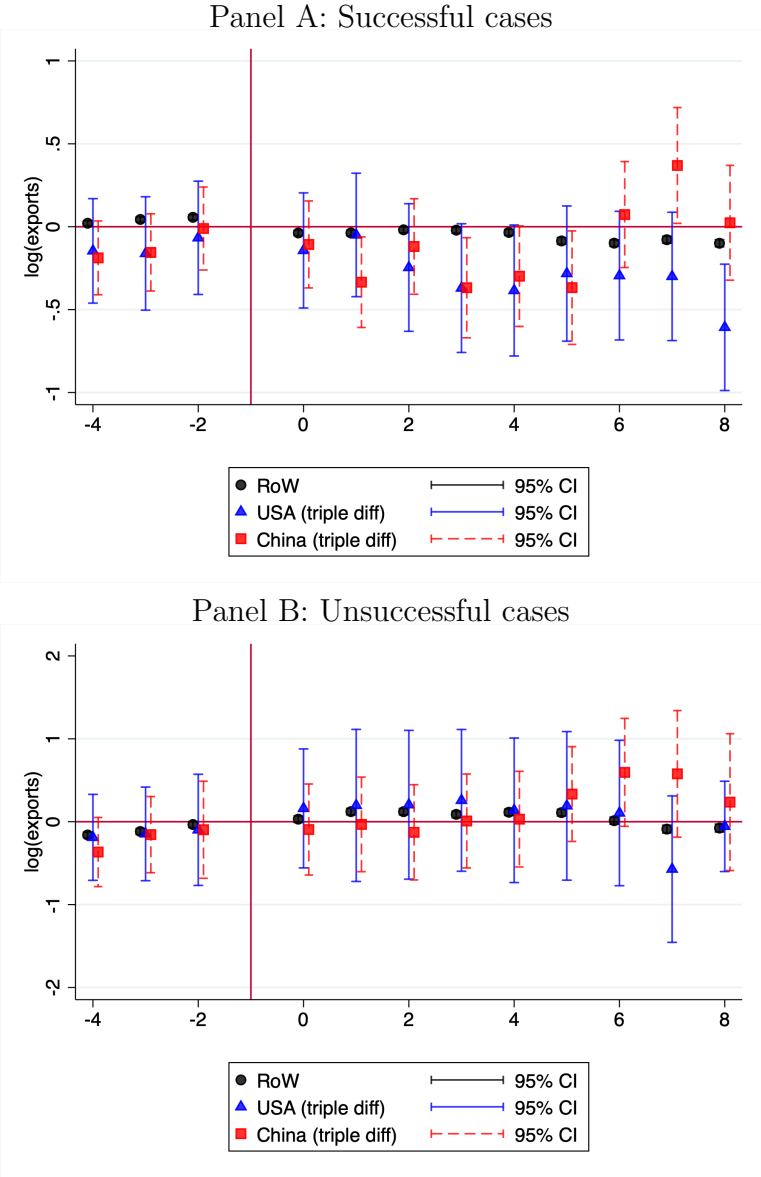


Panel C.2: By HHI, R&D



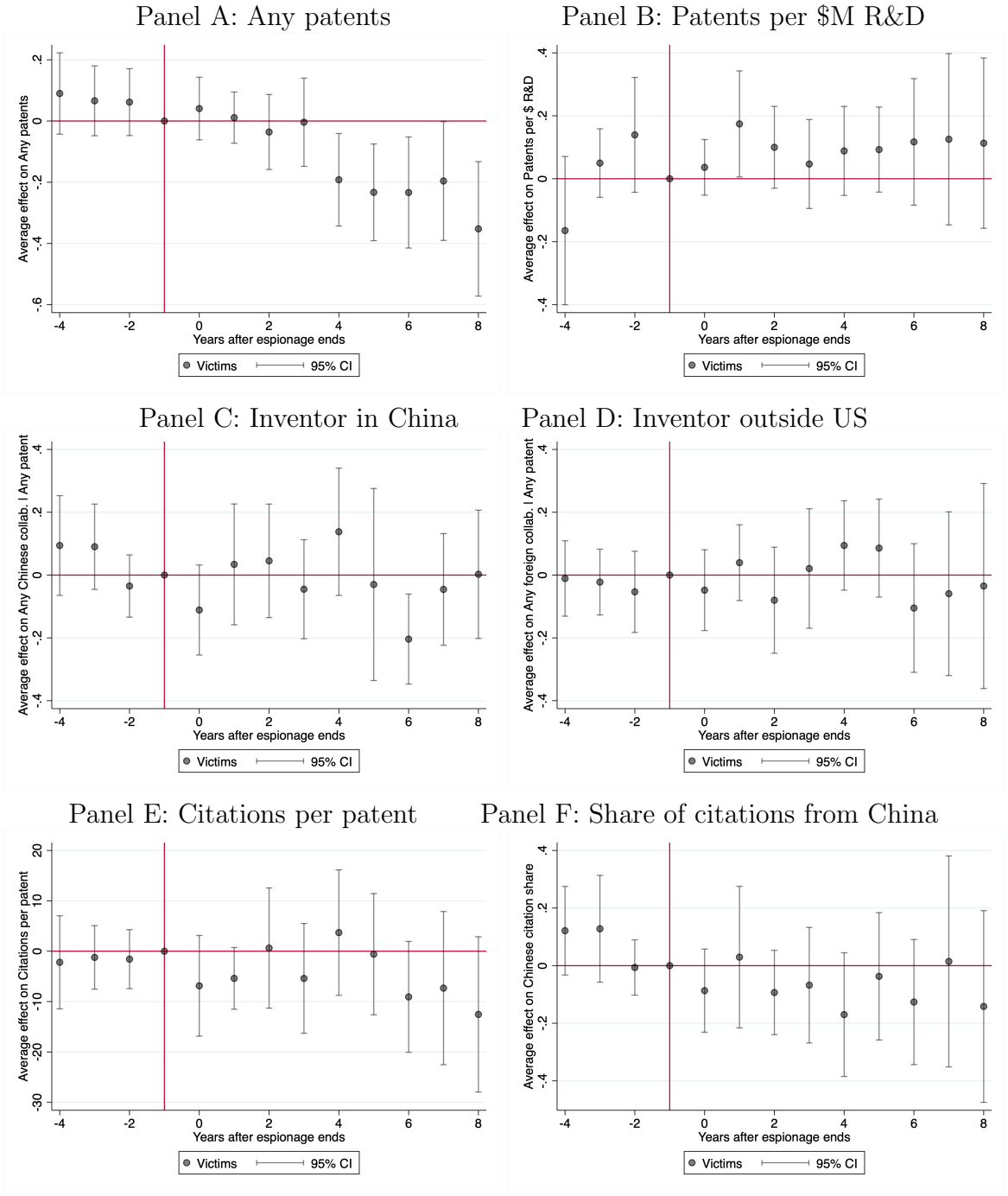
Note: This figure plots heterogeneous effects of espionage incidents. Panel A cuts cases by whether the claimed value of damages in court was above or below the median claimed damage. Panel B cuts cases by whether the targeted firm's industry HHI is above or below the median HHI across industries. Panel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

Figure 6: Effect of espionage on country-level exports



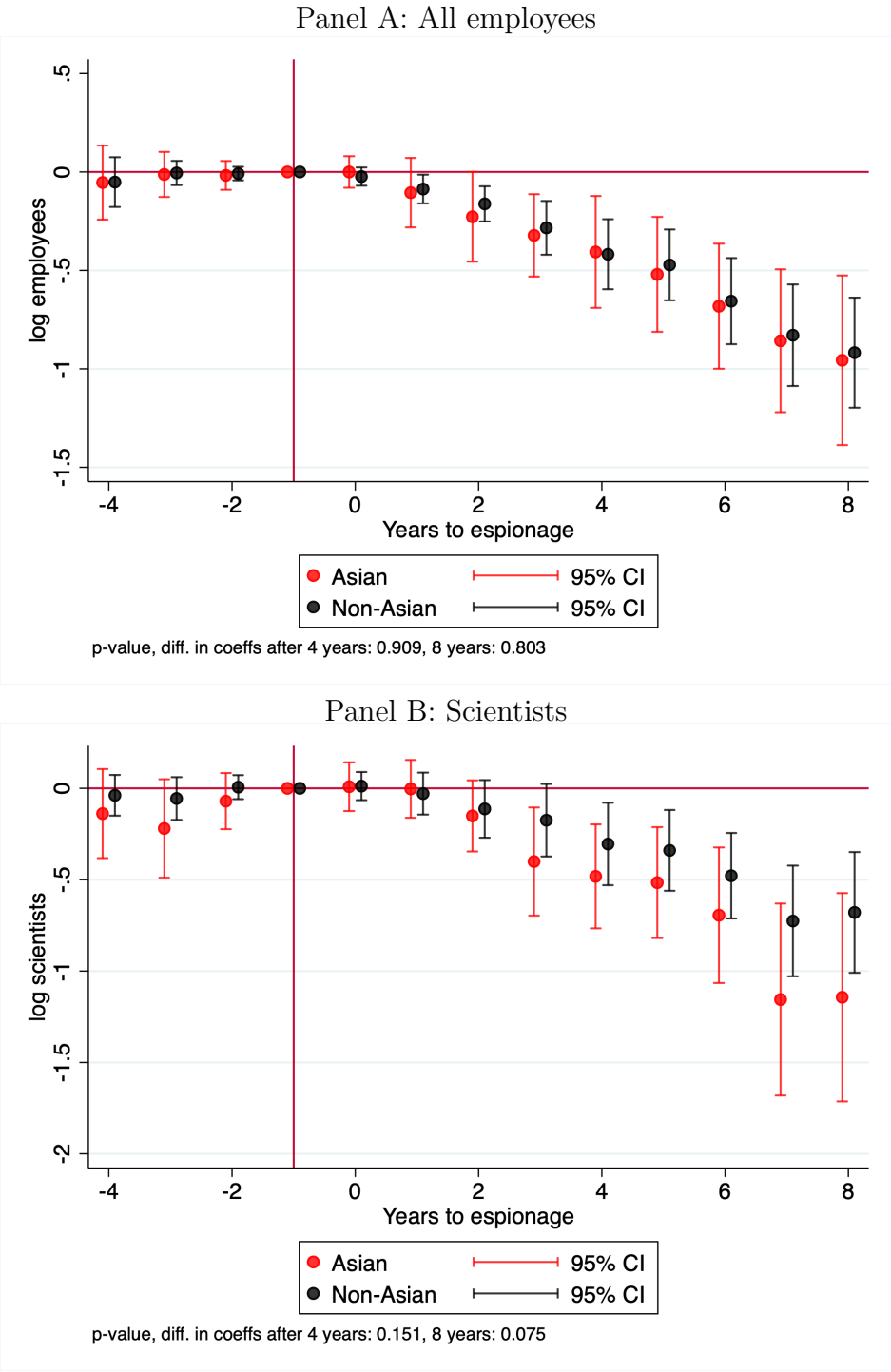
Note: This figure plots coefficients and 95% confidence intervals from a triple differences event study regression at the exporter-year-HS code level. The outcome is the total exports by the exporter in a given year and HS-6 code. The specification includes exporter-year and exporter-HS fixed effects. 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 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. Ethnicity classifications are drawn from name analysis done by Revelio Labs, while scientist job classification is based on job titles. 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.

Table 2: Effect of successful vs. unsuccessful espionage incidents

	log(Revenue)	log(R&D)	log(Assets)	log(Intangible assets)
	(1)	(2)	(3)	(4)
Post espionage X successful	-0.276***	-0.175	-0.158*	-0.366**
	(0.081)	(0.109)	(0.086)	(0.164)
Post espionage X unsuccessful	-0.049	-0.003	-0.019	-0.042
	(0.116)	(0.128)	(0.122)	(0.261)
Post X succ. = Post X unsucc., p-value:	0.0028	0.2743	0.1820	0.0830
Firm FE	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes

Notes: This table presents results from a two-way fixed effects regression at the firm-year level. Post espionage is an indicator for years after (and including) the year when a firm has been targeted for espionage. "Successful" is an indicator for firms targeted by an espionage attempt that succeeded, "unsuccessful" an indicator for firms targeted by an espionage attempt that failed. Standard errors are clustered at the firm level. * significant at 10% ** significant at 5% *** significant at 1%.

Online Appendix

This appendix contains additional material, including figures and tables.

Appendix A Data Cleaning

Appendix A.1 Scientist Job Classification

Revelio Labs categorizes all LinkedIn job titles into 1500 broad jobs. We manually code jobs as being "scientist" jobs based on their title. Alongside any title containing the word "research", the full list of job titles that we classify as scientists are: analytical chemist, automation engineer, CAD designer, CAD engineer, chemical engineer, chemist, clinical research, electrical design engineer, electrical engineering, environmental engineer, environmental scientist, geotechnical engineer, hardware design engineer, hardware engineer, industrial designer, industrial engineer, industrial engineering, innovation, lab, lab tech, lab technician, laboratory, laboratory analyst, laboratory technician, materials engineer, mechanical design engineer, mechanical designer, process developer, process development, process development engineer, process engineer, process engineering, product design, product design engineer, product designer, product developer, product development, product development engineer, product engineer, product engineering, R&D, R&D engineer, R&D project, scientific, scientist, and scientist I.

Appendix A.2 Employee Reviews on Diversity and Inclusion

RevelioLabs provides individual review data for many of the companies in our sample. These reviews include both an individual's overall rating of the company, and also the individual's rating of the company on diversity and inclusion. Additionally, the full text of the employee's review is also recorded.[1] While coverage of the overall ratings and the text of employee reviews range from 2008 to 2025, the diversity and inclusion reviews only begin in 2020. This poses a substantial sample restriction.

To overcome this restriction, we make use of the text of the reviews and natural language processing techniques to impute diversity and inclusion ratings. This allows us to extend coverage of these ratings back to 2008. We use conduct this imputation in two separate ways: TF-IDF and ridge regression, and a fine-tuned BERT model. Heuristically, the TF-IDF and ridge regression method identifies words that are highly predictive of the ratings and uses a penalized regression on these words to estimate the final rating, while the fine-tuned BERT model involves tuning a language transformer model to our particular text corpus to predict the final rating. We describe each method in more detail.

[1] We make use of all text fields available: the review summary, the review advice, the review pros, and the review cons.

TF-IDF and Ridge Regression: We vectorize our training set (data from 2020 onwards) corpus using TF-IDF (term frequency-inverse document frequency). When conducting TF-IDF, we first convert all words to lower case and remove accents. To build the vocabulary of terms, we include both unigrams and bigrams, filter out any terms appearing in over 95% of ratings as stop-words as well as any terms that appear in less than 5 ratings. We also limit the vocabulary to contain a maximum of 300,000 terms. Finally, we use instead of using the raw term frequency, we use $1 + \log(\text{term frequency})$ (sublinear scaling) to smooth the distribution.

With the training set vectorized using TF-IDF, we then run a ridge regression on the diversity and inclusion ratings using $\lambda = 1$ (where λ is the constant on the L2 regularization term). This allows us to fit the model on the training data. To complete the imputation for the full dataset, we vectorize the full dataset and apply the fitted ridge regression model to it.

Fine-tuned BERT model: We begin by splitting the data into 5 folds (with an equal number of companies per fold), splitting the training/test set based on these folds. We next tokenize the text, and use as our baseline model a multilingual BERT (Bidirectional Encoder Representations for Transformers) model fine-tuned for consumer sentiment, `nlptown/bert-base-multilingual-uncased-sentiment` We then fine-tune the model with a regression head to predict the diversity and inclusion rating. To do so, we use the optimizer AdamW with a learning rate of 2e-5, 3 epochs, and a batch size of 8 for both training and evaluation.[2] With the model fine-tuned, we generate predictions for the diversity and inclusion ratings on the full dataset.

On a five point rating scale, we achieve a MAE (mean absolute error) of 0.659 using TF-IDF and ridge regression, and a MAE of 0.728 using the fine-tuned BERT model.

For robustness, we conduct an imputation of the overall ratings using the same methods as the diversity and inclusion ratings. We achieve a MAE of 0.491 using TF-IDF and ridge regression and a MAE of 0.507 using the fine-tuned BERT model. Event study results using overall ratings as the outcome are highly similar regardless of whether we use the actual overall ratings, or the imputed ratings from either method.

Appendix B Additional Analysis

Appendix B.1 Effects on Targeted Firms

Robustness Checks We check whether alternative difference-in-difference estimators yield different results from the baseline specification in Equation 1. In Figure A.2, 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,

[2] We also set the warm-up ratio to 0.1 and use a weight decay parameter of 0.01.

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.

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.3, 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.3, 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.5, 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.

Spillovers within Targeted Industries What happens to other firms in an industry when one of them is targeted for espionage? This could be an identification concern with Equation 1. To address this question, we estimate a triple difference specification using Equation 4. in Figure A.4. Overall, we find no evidence of either positive or negative spillovers to other firms within the same SIC 4-digit code.[3]

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.6 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

[3]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.

[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.

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.6, 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, 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.

Mean Reversion and Industry Dynamics Figure 3 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.7, we show that industry leaders do not systematically mean-revert, especially when we focus on firms targeted by espionage.[6]

A related concern relates to whether industries targeted for espionage look systematically different from other similar industries, and thus may be selected, or simply have differences driven by idiosyncratic industry dynamics. If so, this could affect the interpretation of both industry level regressions (such as the analysis of trade flows), and the assignment of adjacent industries as never-treated firms. 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 differences in the persistence of industry leadership (columns 1-4), size difference between top firms (column 5), or HHI (column 6) between them.

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

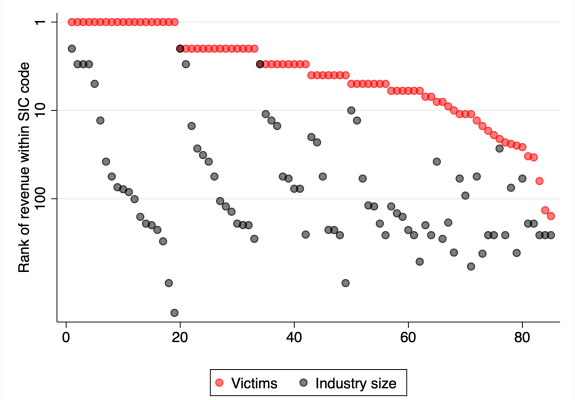
[6]Industry leadership is highly autocorrelated, and the average leader firm targeted by espionage has already been a leader for over 15 quarters by the time they are targeted.

Appendix C Additional Tables and Figures

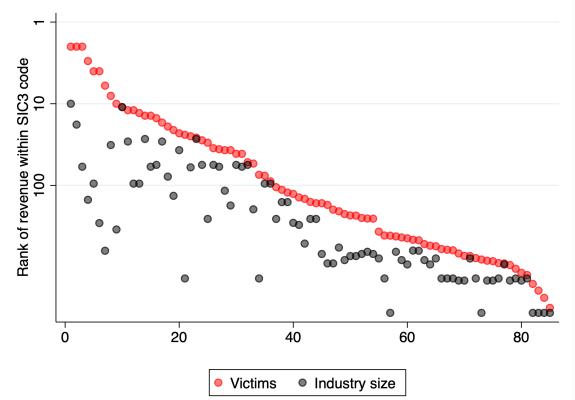
Figure A.1: Rank of victim firms by size within industry

Panel A: Revenue

Panel A.1: Industry is SIC

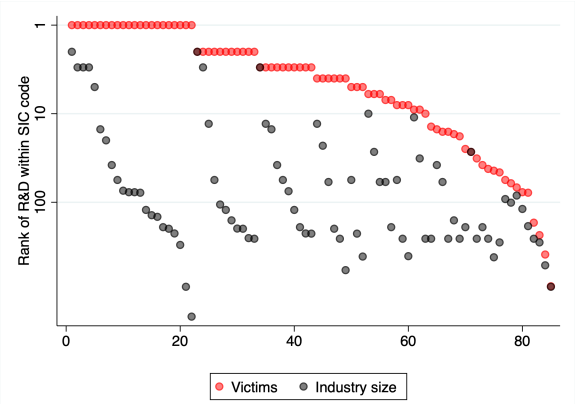


Panel A.2: Industry is SIC3

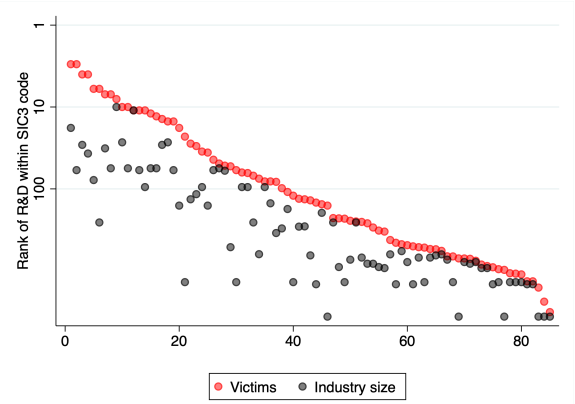


Panel B: R&D expenditures

Panel B.1: Industry is SIC



Panel B.2: Industry is SIC3

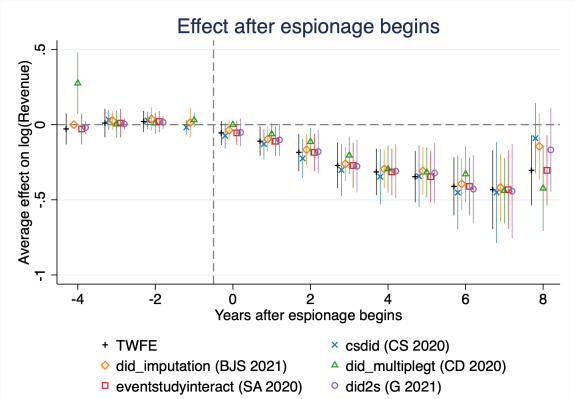


Note: This figure plots the rank of victim firms by size within their industry in red, and the size of their industry in gray. In Panels A and B, revenue is used as an indicator for firm size. In Panels C and D, R&D expenditures are used as an indicator for firm size. In Panels A and B, a firm's industry 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.

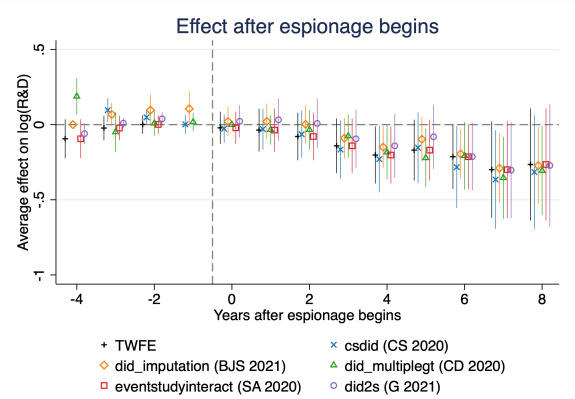
Figure A.2: Effect of espionage on victim firm's log revenue and R&D expenditures, alternate heterogeneous DID estimators

Panel A: Successful cases

Panel A.1: log(Revenue)

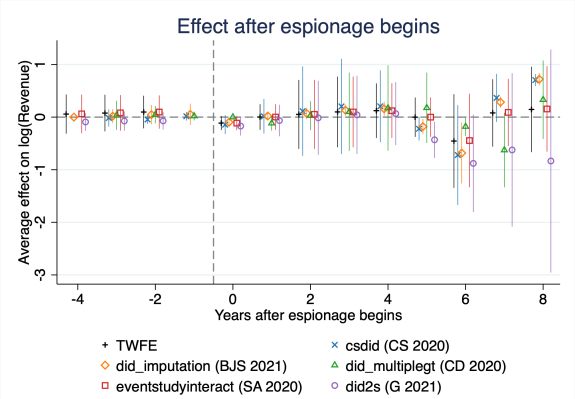


Panel A.2: log(R&D)

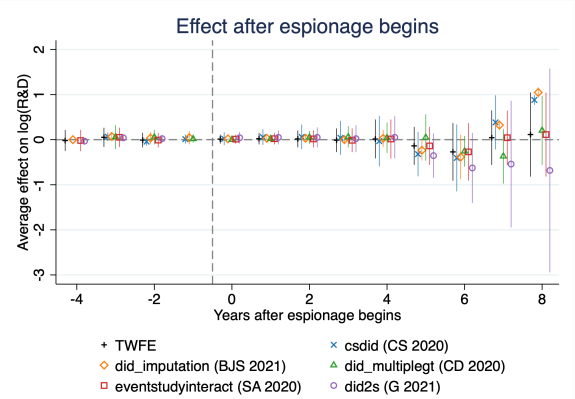


Panel B: Unsuccessful cases

Panel B.1: log(Revenue)

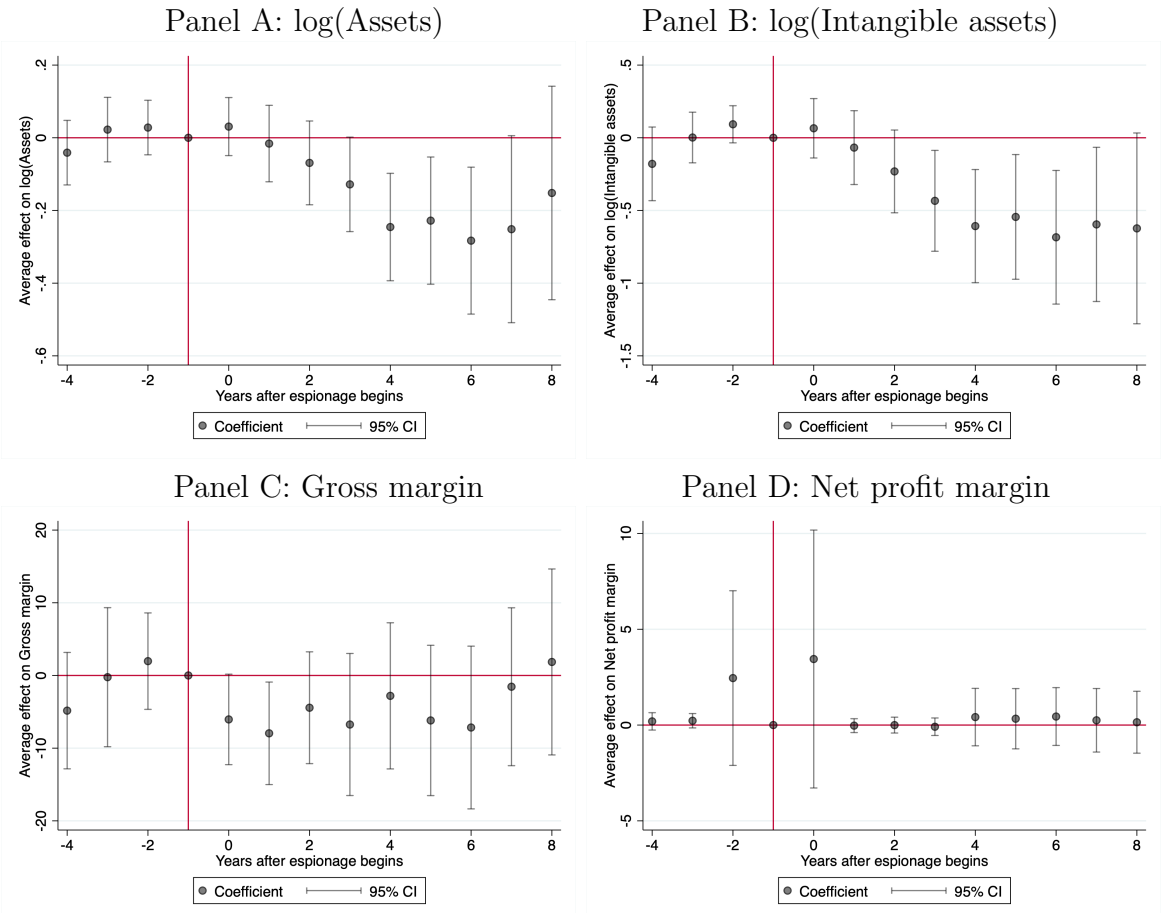


Panel B.2: log(R&D)



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 Chaisemartin 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.3: Effect of espionage on secondary firm outcomes

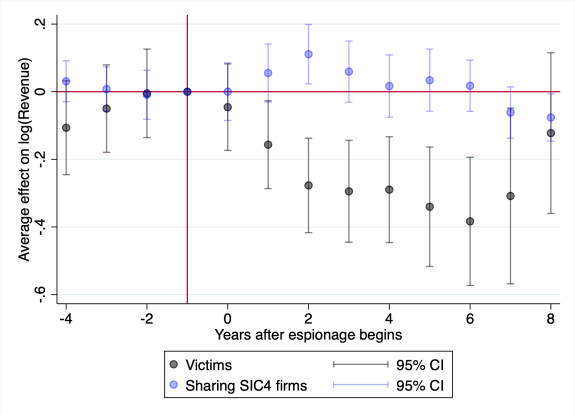


Note: This figure plots coefficients and 95% confidence intervals from various heterogeneous dynamic difference-in-difference specifications. An event is a firm being successfully targeted for economic espionage. The outcome in Panels A is a firm's log(Assets), in Panel B a firm's log(Intangible assets), in Panel C a firm's gross margin, and in Panel D a firm's net profit margin.

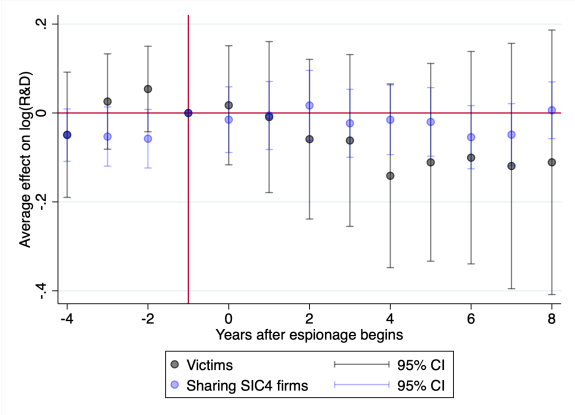
Figure A.4: Effect of espionage on victims and other firms in the same industry, log revenue and R&D expenditures

Panel A: Successful cases

Panel A.1: log(Revenue)

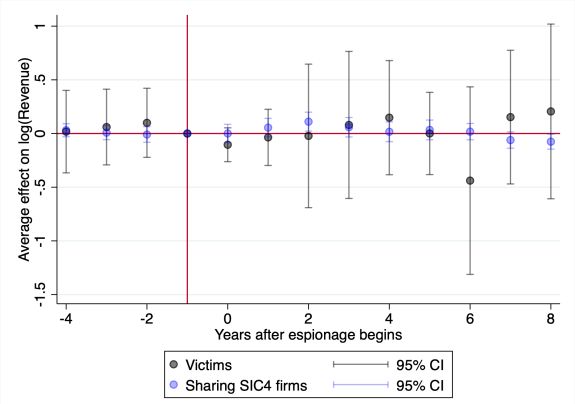


Panel A.2: log(R&D)

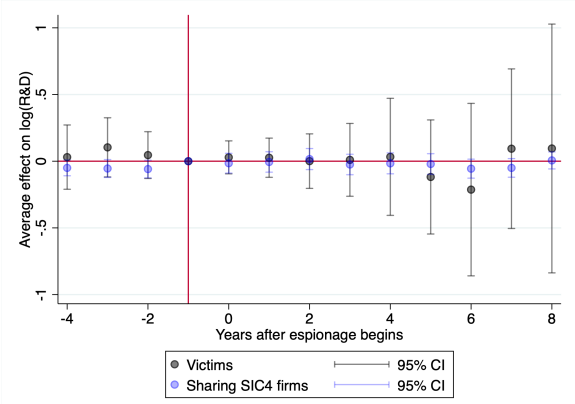


Panel B: Unsuccessful cases

Panel B.1: log(Revenue)

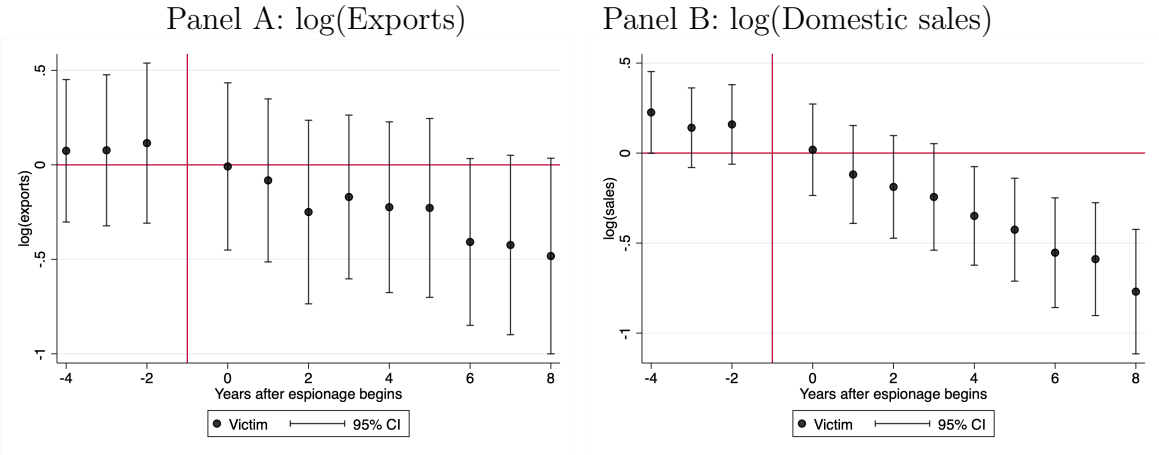


Panel B.2: log(R&D)



Note: This figure plots coefficients and 95% confidence intervals from a 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 A.5: Effect of espionage on victim firm log exports and domestic sales

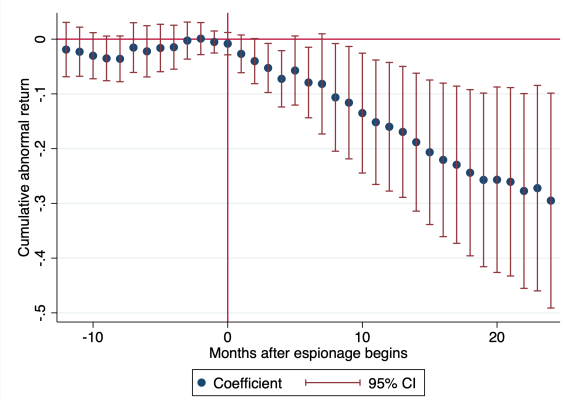


Note: This figure plots coefficients and 95% confidence intervals from a two-way fixed effects event study regression. An event is a firm being successfully targeted for economic espionage. The outcome in Panel A is a firm's log(Exports) and in Panel B a firm's log(Domestic sales). The unit of analysis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

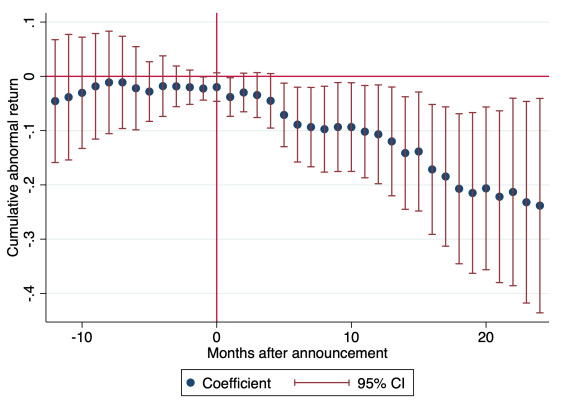
Figure A.6: Effect of espionage on victim firm's cumulative abnormal returns

Panel A: Successful cases

Panel A.1: After espionage begins

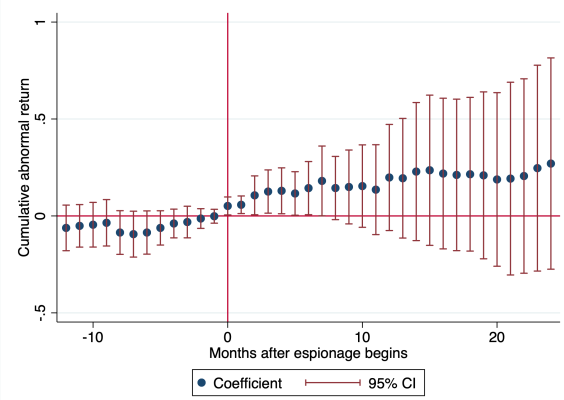


Panel A.2: After publicly announced

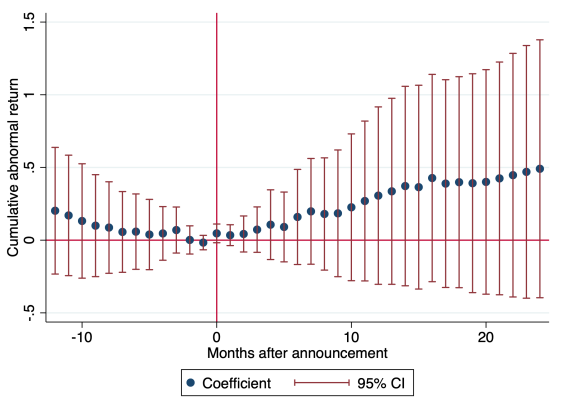


Panel B: Unsuccessful cases

Panel B.1: After espionage begins

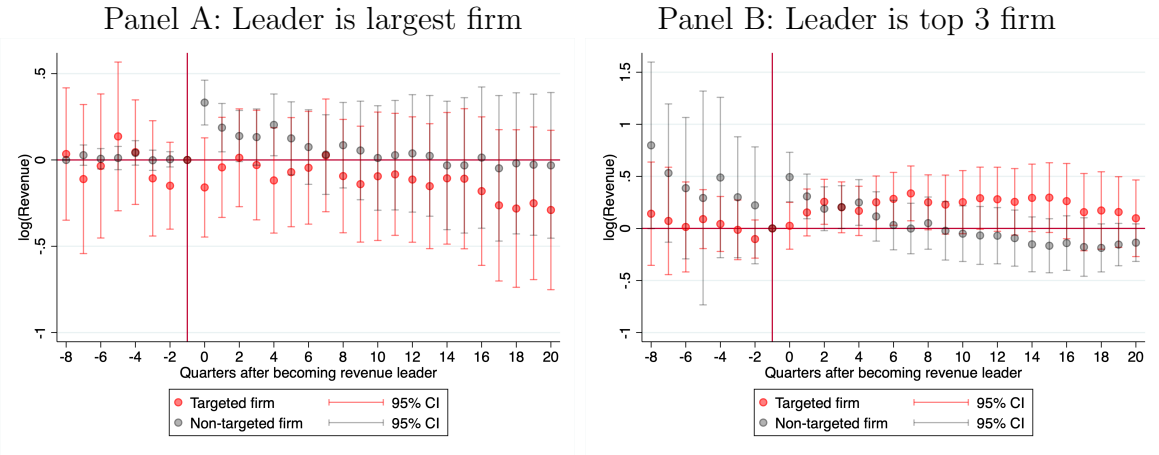


Panel B.2: After publicly announced



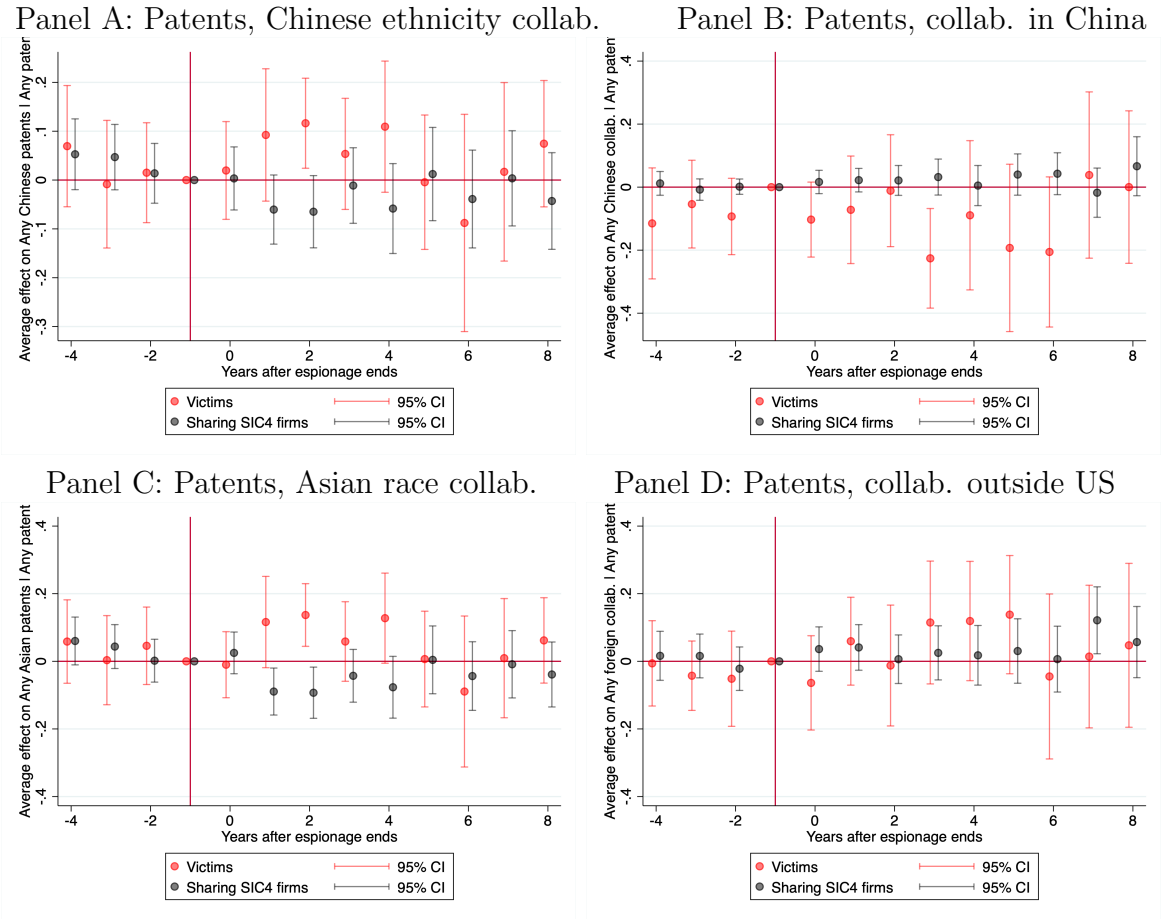
Note: This figure plots coefficients and 95% confidence intervals from regressions on victim firms of economic espionage at various time horizons. In Panel A, an event is a firm being successfully targeted for economic espionage. Panel A.1 uses the timing of when espionage begins (an agent first begins 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.7: Firm log revenue in the quarters preceding and following when they become an industry leader



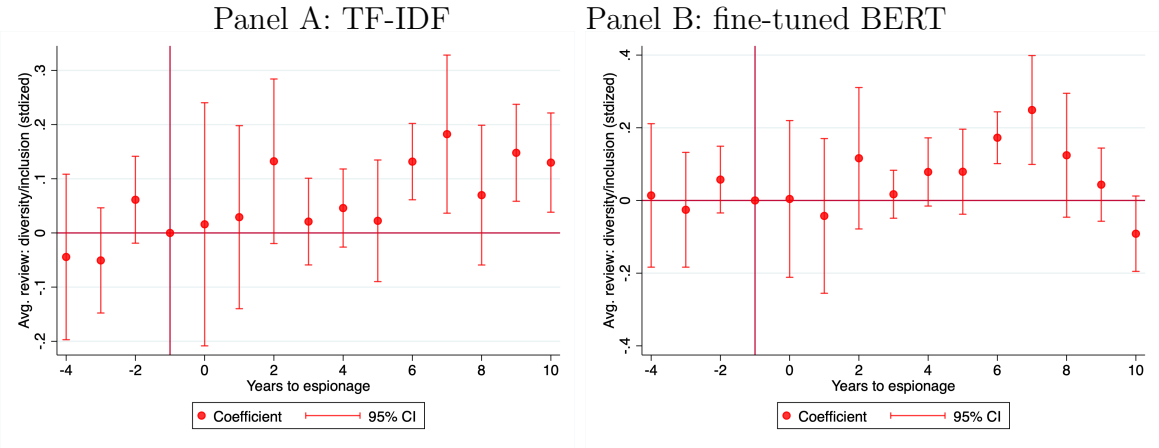
Note: This figure plots coefficients and 95% confidence intervals from two-way fixed effects event study regressions. An event is a firm becoming a leader in their industry (SIC-4). In Panel A, a leader is defined as the largest firm by revenue. In Panel B, a leader is defined as a top three firm by 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.8: Effect of espionage on proportion of patents with foreign collaborators, spillovers to industry



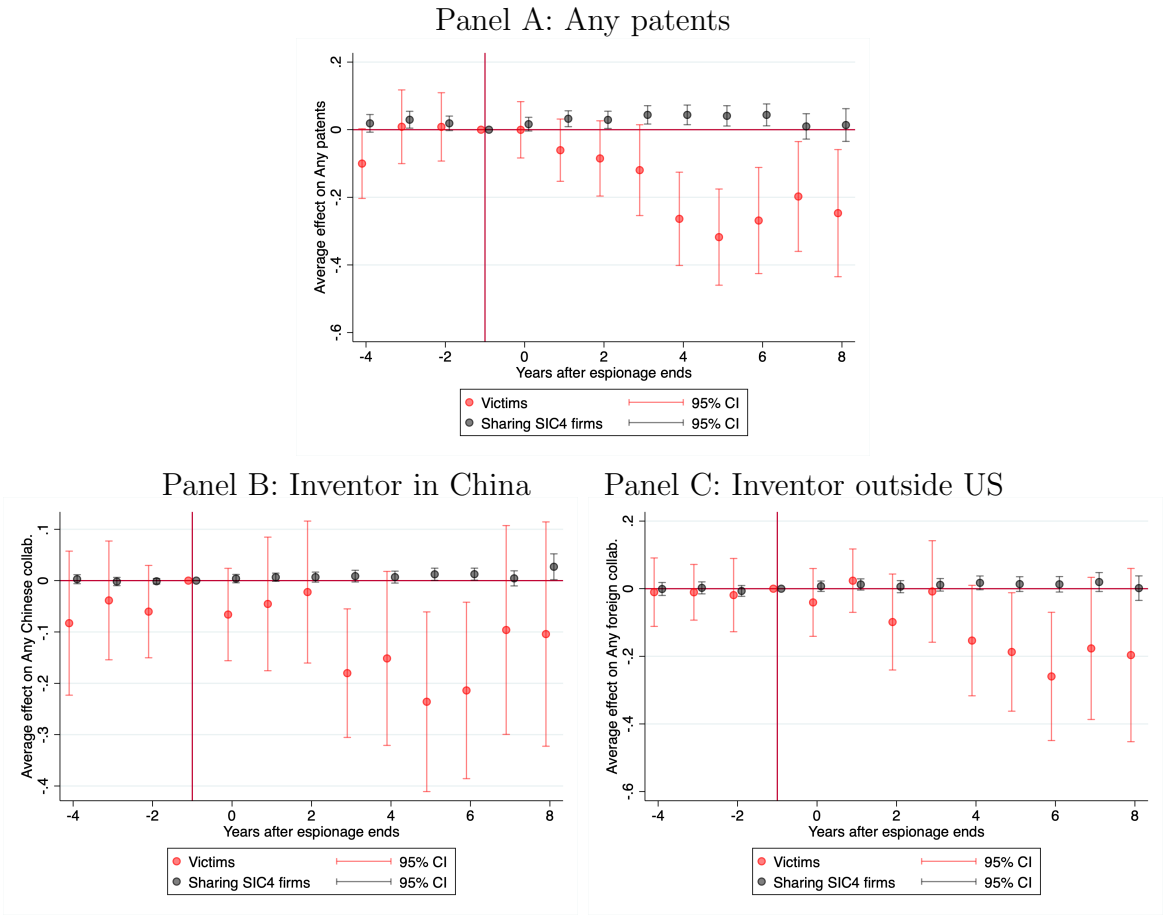
Note: This figure plots coefficients and 95% confidence intervals from a triple differences two-way fixed effects regressions. An event is when an successful economic espionage incident ends. The outcome in Panel A is whether the firm patented with an ethnic Chinese co-author, in Panel B whether the 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 corporate diversity/inclusion measures



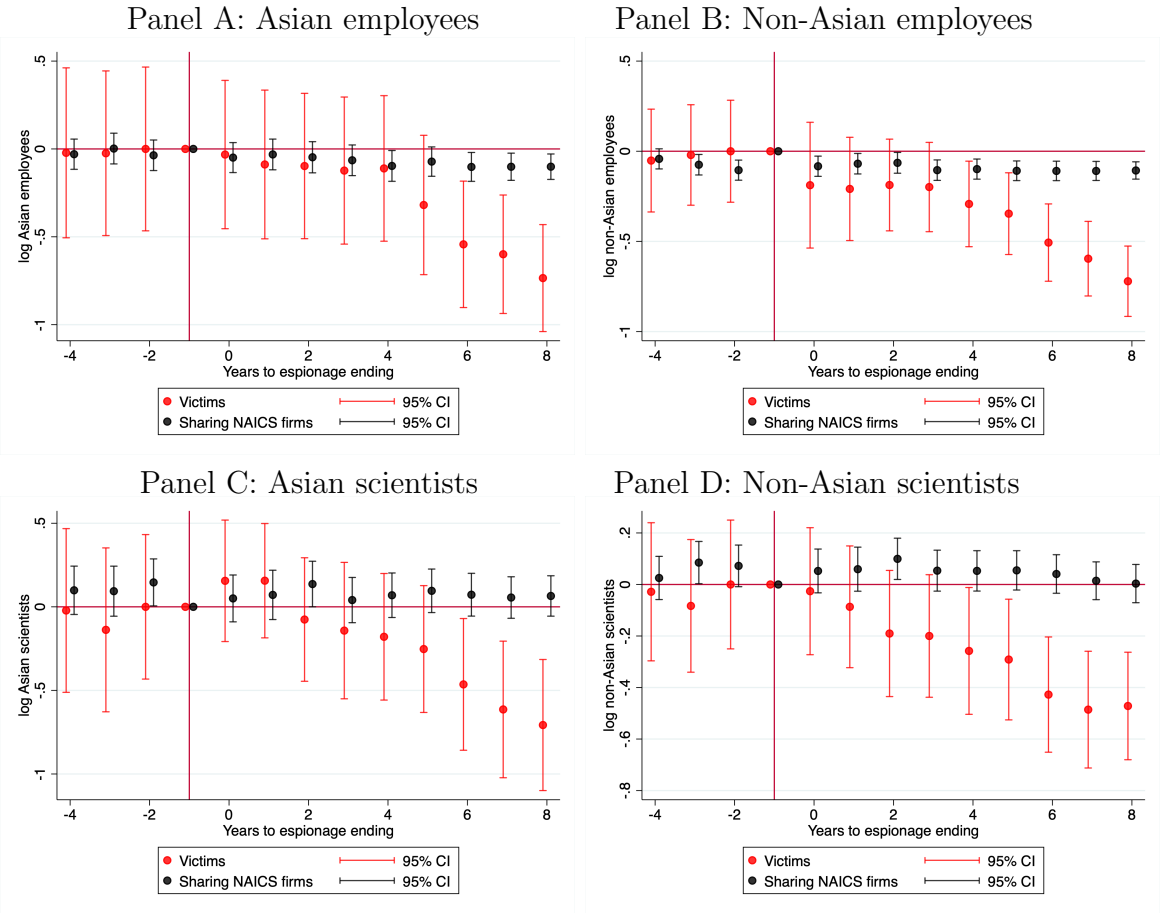
Note: This figure plots coefficients and 95% confidence intervals from two-way fixed effects regressions. Each unit is a firm. The outcome is a measure computed from the text of employee reviews, whose construction is detailed in Appendix Appendix A.2.

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



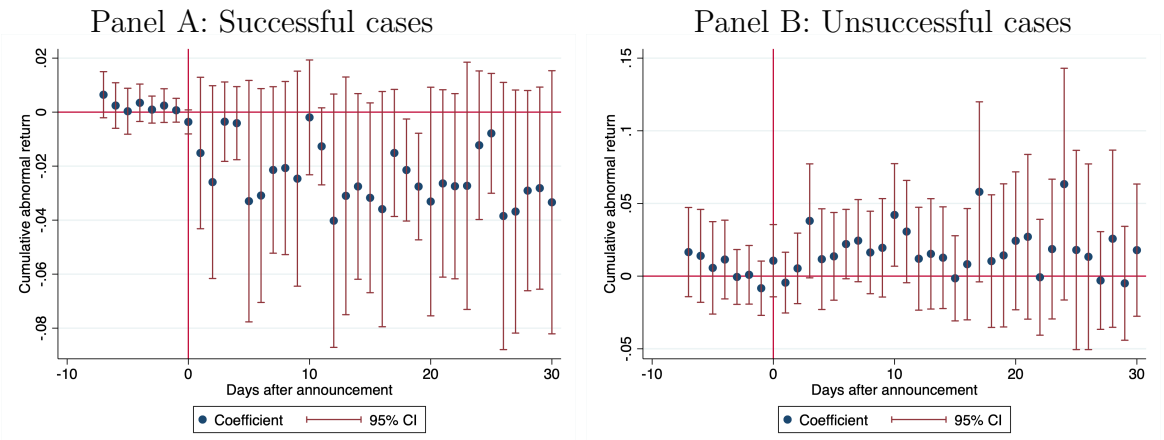
Note: This figure plots coefficients and 95% confidence intervals from triple-difference two-way fixed effects regressions. An event is when an successful economic espionage incident ends. The outcome in Panel A is whether the firm patented in a given year, in Panel B whether the firm patented with an 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: 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.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%.