Business and Politics (2025), **27**, 95–113
doi:10.1017/bap.2024.22

CAMBRIDGE UNIVERSITY PRESS

RESEARCH ARTICLE

State-sponsored cyber attacks and co-movements in stock market returns: evidence from US cybersecurity defense contractors

William Akoto

Department of Foreign Policy & Global Security, School of International Service, American University, NW Washington, DC, USA
Email: william@willakoto.com

Abstract

State-sponsored cyber attacks are increasingly attracting attention in the literature, with many analysts interested in the firm-level economic implications of these attacks. Nevertheless, the bulk of these studies focus on firms directly targeted in the attacks. In this paper, I examine the broader, often overlooked ripple effects of these attacks on third-party entities like cybersecurity service providers who are frequently at the frontlines of dealing with these attacks. Leveraging data on cyber attacks and stock market returns for a sample of U.S. based cybersecurity defense contractors from 2000 to 2020, I empirically demonstrate that an escalation in the intensity of state-sponsored cyber attacks prompts a behavioral shift among investors and regulators, leading to increased co-movement in firms' stock returns. This paper thus adds a novel dimension to our understanding of the complex interplay between state-sponsored cyber attacks and the market dynamics of cybersecurity defense contractors, with important implications for national cybersecurity.

Keywords: cyber conflict; cybersecurity service providers; state-sponsored cyber operations; stock market integration

Introduction

As cyber threats become increasingly central to international politics, state-sponsored cyber attacks have become an instrument of geopolitical leverage. Emerging evidence shows that states are increasingly turning to cyber industrial espionage to boost the competitiveness of domestic firms.[1] These sophisticated and well-orchestrated attacks often target critical infrastructure systems and sensitive data, with severe ramifications for the targeted firms and the national economy.

Recognizing this, scholars are increasingly paying attention to how cyber attacks can impact the stock market. Stock markets are not only essential to the firms that trade in these markets but also play a pivotal role in the national economy by serving as a conduit for various economic activities. Stock markets facilitate the raising of capital by companies through the issuance of shares to the public. This capital is then used for expansion, research and other corporate activities, which in turn contribute to economic growth. Stock markets also play a vital role in determining the prices of securities through the mechanisms of supply and demand. This process is essential for the efficient allocation of resources in the economy. Moreover, publicly traded companies are subject to regulations which can lead to better corporate governance practices. This can have positive effects on other facets of the national economy. Stock markets are thus integral to the functioning and development of the economy and overall economic stability and growth.

Studies that examine the nexus between state-sponsored cyber attacks and stock market dynamics primarily focus on the immediate victims of such attacks, finding a negative effect on stock returns, shareholder wealth and innovation levels of targeted firms in the immediate period following the

[1]Akoto (2022).

© The Author(s), 2024. Published by Cambridge University Press on behalf of Vinod K. Aggarwal. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

https://doi.org/10.1017/bap.2024.22 Published online by Cambridge University Press

attacks.[2] However, the focus on firms directly targeted by cyber attacks invariably overlooks the ripple effects of these attacks on third-party organizations such as cybersecurity service providers. I address this issue in this paper. I pay articular attention to cybersecurity defense contractors—firms that provide cybersecurity solutions to the military and government agencies.

Studying the third-party effects of cyber attacks on these firms is critically important because they play a pivotal role in securing national digital infrastructures and safeguarding sensitive state information. Any disruption or instability in their economic health could potentially compromise a nation's cyber defense capabilities. Furthermore, as these firms are intricately tied to a nation's security apparatus, their perceived vulnerability or resilience can influence national security perceptions both domestically and internationally. A weakened confidence in these contractors, as reflected by their stock performance, can send signals to adversarial states about potential vulnerabilities in the nation's cyber defenses. This could embolden adversaries to ramp up their cyber operations, believing the nation to be more susceptible to cyber intrusions and attacks. Additionally, the financial stability of these contractors influences their capacity to invest in research, development and innovation—key components to staying ahead in the constantly evolving cyber domain. Thus, understanding the market reactions and consequential effects on cybersecurity defense contractors in the aftermath of state-sponsored cyber attacks provides insights not just into economic ramifications, but also into broader national security implications.

Within this context, I examine how the severity of state-sponsored cyber attacks affects co-movement in the stock returns of a sample of cybersecurity defense contractors. At its core, co-movement in stock returns refers to the synchronized rise and fall in stock prices of different firms. When stocks co-move, it signifies that market forces or external events are influencing them in a similar manner, regardless of their individual characteristics. Furthermore, co-movement is closely tied to the concept of market integration. When firms' stocks co-move consistently, it suggests a high degree of market integration. This implies that information (or shocks) are rapidly and uniformly disseminated across the market, affecting all integrated firms similarly.[3] For cybersecurity defense contractors, increased co-movement can indicate that the market perceives these firms as a collective unit, especially in response to cyber threats or state-sponsored attacks. It underscores the market's view of the industry's collective vulnerability to such threats or the opportunities therein.

I develop a novel theoretical framework that links the severity of state-sponsored cyber attacks to the homogenization of cybersecurity investments by defense contractors in the aftermath of cyber attacks and changes in the regulatory environment confronting these firms. These changes shift investor sentiments towards viewing these firms as a homogeneous group subject to similar risks and opportunities.

For instance, consider a major cyber attack attributed to a state actor, targeting critical infrastructure. In the immediate aftermath, as media reports and official statements highlight the sophistication and impact of the attack, there's a growing public and governmental awareness of cybersecurity vulnerabilities. Investors, foreseeing a surge in demand for cyber security solutions, are likely to increase their stakes in firms providing these services. This investor behavior is driven by the expectation of future contracts and business expansions for these firms as governments and corporations seek to fortify their digital defenses against similar threats. In this case, stock returns of cybersecurity companies might increase in response to the cyber attack.

Conversely, there are scenarios where cybersecurity company stocks might experience a decline following a cyber attack. For example, consider a major cyber attack where a cyber security firm's solutions are implicated in failing to prevent the attack. For instance, a case where a state-sponsored cyber attack successfully breaches the defenses of a major corporation, despite the corporation employing the latest cybersecurity solutions from a well-known provider.

In the aftermath of such an attack, media scrutiny and public discourse might focus on the inadequacy of the cybersecurity firm's products or services in thwarting the breach. This negative attention can erode investor confidence in the firm's capabilities, leading to a perception that the

[2]Gatzlaff and McCullough (2010); He, Frost and Pinsker (2020); Kamiya et al. (2018).
[3]Baillie and DeGennaro (1990).

https://doi.org/10.1017/bap.2024.22 Published online by Cambridge University Press

company may not be as resilient or effective against sophisticated cyber threats as previously believed. Concerns about potential loss of existing clients, difficulty in acquiring new contracts and potential legal liabilities can further exacerbate this sentiment. Investors, reacting to these developments and the potential impact on the firm's future revenue and reputation, might begin to divest their holdings in the cybersecurity company. This sell-off can extend to other firms in the sector as investors reassess the overall efficacy and reliability of cybersecurity solutions in the face of evolving and sophisticated state-sponsored cyber threats. The market's reaction, in this case, is driven not by the anticipation of increased demand but by doubts over the sector's ability to effectively counter high-level cyber threats. In both scenarios, cybersecurity firms are likely to experience a collective movement (positive in the first, negative in the second) in their stock returns.[4,5]

Within this context where cybersecurity company stocks may co-move in the aftermath of a cyber attack, I leverage datasets of state-sponsored cyber attacks and stock market returns for a sample of cybersecurity defense contractors to document a strong robust association between increased severity of state-sponsored cyber attacks and increased stock return co-movement over the period 2000–2020.

This finding matters for the existing literature in three important ways. First, it highlights the fact that the economic repercussions of state-sponsored cyber attacks are not confined only to the direct targets of these attacks. The evidence suggests a broader and more systemic impact, underscoring the interconnectedness of the modern economic landscape and its susceptibility to cyber threats. Second, by highlighting the co-movement in stock returns of cybersecurity defense contractors, it underscores the market's collective sentiment and perception of the entire cybersecurity sector in the wake of cyber attacks. This has implications for understanding investor behavior and the overall confidence in the cybersecurity industry's ability to counter state-sponsored threats. Lastly, the results offer a novel perspective on the indirect strategic implications of cyber warfare. If adversarial states recognize that their cyber operations can influence the stock market dynamics of key defense contractors, it could become a deliberate strategy to weaken a nation's cyber defense capabilities, both economically and operationally, thereby opening up a new front in the realm of cyber strategic warfare.

The findings also have important implications for national security. For one, many critical infrastructure systems such as energy, transportation and communications networks are heavily reliant on cybersecurity solutions provided by these firms. If they are financially impacted due to co-movement in stock returns, their ability to protect these critical infrastructures could be diminished, posing direct threats to national security. The co-movement in stock returns can also affect the allocation of national economic resources. For example, if there is a sharp decline in cybersecurity stocks due to an increase in cyber threats, the government might be forced to allocate more resources to bolster national cybersecurity.

To illustrate, consider the case of a cybersecurity firm which specializes in providing advanced security solutions to federal agencies. Its financial health is closely tied to its stock performance, as many of its expansion and R&D initiatives are funded through capital raised in the stock market. In a scenario where there's a significant cyber attack that exposes vulnerabilities in its systems investor confidence could wane, resulting in a sharp decline in its stock returns (and potentially those of similar cybersecurity defense contractors). As the firm's market value plummets, it finds itself with reduced financial resources. Consequently, it might need to scale back its R&D spending or delay the expansion of critical security infrastructure projects.

This reduction in investment could leave critical government cyber infrastructure more vulnerable to cyber attacks. In response to this heightened risk, the government might find it necessary to intervene. This could involve direct financial injections into the cybersecurity defense sector, increased subsidies for cybersecurity solutions or even the establishment of government-led projects to develop

[4]Baillie and DeGennaro (1990).

[5]While the stock price is the cost of purchasing a share of a company on the open market, stock returns refer to the gain or loss made from investing in a stock over a certain period of time. This can be in the form of capital gains (or losses) and/or dividends. Capital gains occur when the stock price increases between the time an investor buys it and when they sell it. Dividends are a portion of the company's earnings that are distributed to shareholders. The total return on a stock is the sum of capital gains and dividends.

https://doi.org/10.1017/bap.2024.22 Published online by Cambridge University Press

and implement necessary cybersecurity technologies and protocols. Such governmental intervention is not only costly but may also come at the expense of investments in other areas such as education or healthcare. Moreover, negative co-movement in stock returns can affect public confidence in the government's ability to protect citizens from cyber threats. This might lead to social unrest or affect the democratic process.

I also compare the effect of cyber attack severity for cybersecurity defense contractors with the effect on mainstream traditional cybersecurity firms, who typically serve private sector businesses and the general public. In this case, the severity of cyber attacks does not have a clear, significant impact on the level of market integration among the sampled cybersecurity service providers. This suggests that there might be significant differences in the way investors respond to cyber attacks affecting clients of these two groups. This underscores the need for nuanced strategies to address cybersecurity challenges, tailored to the distinct roles and market expectations surrounding cybersecurity defense contractors and mainstream cybersecurity service providers.

In the sections that follow, I situate this work in the broader cyber politics literature and then present my theoretical framework. I then present an analytical framework to examine the effect of cyber attack severity on the stock returns of a representative sample of cybersecurity defense contractors. The results and conclusions follow that.

State-sponsored cyber attacks and market dynamics

In the burgeoning field of cyber politics, understanding the multifaceted impacts of state-sponsored cyber operations is increasingly paramount. State-sponsored cyber attacks occupy a distinctive and notably pernicious niche within the realm of cyber threats. Unlike non-state actors, nation-states can marshal substantial technical, financial and intelligence resources towards developing and deploying cyber operations that target adversaries' digital assets and infrastructures.[6] The strategic imperatives underpinning these operations often extend beyond immediate objectives to encompass broader geopolitical and strategic agendas. This makes state-sponsored cyber attacks a vital instrument of statecraft in the digital age.[7]

Pioneering works in the study of state-sponsored cyber attacks have primarily focused on the direct targets of cyber attacks, shedding light on the immediate strategic, economic and political implications of these incidents.[8] These studies often emphasize the immediate disruptions caused by cyber attacks, from data breaches and infrastructure sabotage to intellectual property theft and espionage.

While this focus on direct targets provides invaluable insights, a nascent yet growing body of literature has begun to explore the ripple effects of cyber operations. These works recognize that in an interconnected digital ecosystem, the consequences of cyber attacks often cascade beyond the primary targets to impact a broader array of entities and sectors. For instance, research has highlighted why cybersecurity is a key national security issue,[9] how cyber incidents can shape global financial markets[10] and even impact diplomatic relations between countries.[11]

Cyber attacks also pose a serious threat to national security due to their direct impact on critical infrastructure systems that sustain national economic stability and public safety. These attacks might target vital sectors such as energy, finance, healthcare, and transportation, disrupting operations, compromising sensitive data, and potentially causing widespread economic and physical damage. The interconnected nature of these systems means that a breach in one can lead to cascading failures across multiple sectors, amplifying the threat to economic stability and public well-being.[12]

[6]Buchanan (2016).
[7]Nye (2014).
[8]Buchanan (2016); Gartzke and Lindsay (2015); Valeriano and Maness (2014).
[9]Cavelty (2010).
[10]Amir, Levi and Livne (2018).
[11]Attatfa, Renaud and De Paoli (2020).
[12]Valeriano and Maness (2015).

https://doi.org/10.1017/bap.2024.22 Published online by Cambridge University Press

Moreover, cyber attacks undermine business confidence and can lead to significant financial losses, both of which deter investment and innovation. When businesses are attacked, they must divert resources to recovery and defense, rather than growth or innovation, stifling economic progress. In the face of such threats, the government often has to increase its expenditure over time to bolster cybersecurity defenses and aid affected sectors, straining public resources and shifting attention from other critical national needs. This economic disruption and the subsequent governmental response underscore the significant national security risks posed by cyber attacks.[13]

In this evolving discourse, the economic dimensions of state-sponsored cyber attacks have garnered increasing attention. Scholars have begun to explore how cyber incidents influence stock market behaviors, investor sentiments and overall market dynamics.[14] Much of this literature, however, remains confined to understanding the immediate market reactions to firms directly targeted by cyber attacks, often revealing negative stock performance in the aftermath of such incidents.[15]

In this paper, I complement these existing studies by turning attention to the third-party effects of state-sponsored cyber attacks, specifically on cybersecurity defense contractors. As highlighted earlier, these are firms that provide cybersecurity solutions to the military and government agencies. Examples include mainstream cybersecurity firms such as FireEye, CrowdStrike and Palo Alto Networks. It also includes companies like Lockheed Martin, Northrop Grumman and Booz Allen Hamilton who traditionally provide defense contracting services to militaries and government agencies but have recently added cybersecurity services to their repertoire. These range from threat intelligence and analysis to the development and implementation of advanced cybersecurity technologies. These firms are thus increasingly becoming essential in ensuring the cybersecurity of critical national infrastructures, sensitive data and vital government operations. The stability, efficiency and resilience of cybersecurity defense contractors is thus intricately linked with a nations cybersecurity health and its ability to safeguard against external and internal cyber threats.

While the cybersecurity industry's role in national defense and global cyber politics has been acknowledged in literature, limited attention has been given to understanding how the cascading effects of state-sponsored cyber attacks affects the market dynamics of these firms. By focusing on the co-movement in stock returns of cybersecurity defense contractors in the wake of state-sponsored cyber attacks, I contribute to the literature by introducing a novel perspective on understanding the broader economic repercussions of cyber incidents. This extends the current discourse beyond directly affected firms. I also help bridge the often-separated domains of cyber politics, economics and international relations, offering a more holistic view of the impact of state-sponsored cyber operations.

Theoretical framework

I argue that a rise in the severity of state-sponsored cyber attacks leads to the homogenization of cybersecurity investments and the regulatory environment confronting cybersecurity defense contractors. This induces stock market investors to view these contractors as a homogeneous group facing similar risks and opportunities. This behavioral shift on the part of investors causes the stocks of contractors to move in tandem, increasing the market integration of these firms with each other.

To start, state-sponsored cyber attacks are generally characterized by a high level of sophistication.[16] The involvement of state actors means that these attacks are frequently well-funded, meticulously planned and executed with a level of expertise that is significantly better than that of typical cyber criminals.[17] This relative endowment enables state-sponsored cyber actors to exploit vulnerabilities in networks and systems that may have been previously unknown or unaddressed. Severe attacks can compromise critical infrastructure or highly sensitive data and have consequences that reach far beyond the targeted entity.

[13]Akoto (2022).
[14]Gatzlaff and McCullough (2010); He, Frost and Pinsker (2020); Kamiya et al. (2018).
[15]He, Frost and Pinsker (2020); Kamiya et al. (2018).
[16]Rid and Buchanan (2015).
[17]Blinderman and Din (2017).

https://doi.org/10.1017/bap.2024.22 Published online by Cambridge University Press

First, cybersecurity firms may incur damages to their reputation in the wake of cyber attacks, particularly if their clients are targeted. An example is the reputational losses suffered by cybersecurity firm SolarWinds in the wake of an alleged Russian state-sponsored cyber attack on its clients in 2020. In this attack, malicious code was inserted into the updates of SolarWinds' Orion software. This tainted software was then subsequently installed by thousands of the company's clients, giving the attackers access to their networks.[18]

Subsequent to the attack, SolarWinds was heavily criticized for lax cybersecurity practices that made the attack possible.[19] This incident also had industry-wide repercussions. The realization that a state-sponsored actor could infiltrate the defenses of a premier cybersecurity company signaled to other cybersecurity firms the need to bolster their own defenses.[20] This led them to invest in similar cutting-edge technologies to bolster their defenses.[21] Successful cyber attacks are thus often perceived as a clarion call for cybersecurity firms to fortify their defense systems.[22]

Second, successful cyber attacks signal to entities that they must be circumspect and diversified in their cybersecurity postures, not relying solely on the protections afforded by any single cybersecurity provider.[23] Consequently, the demand for cybersecurity services tends to go up after an attack.[24] These companies also often face increased customer pressure to invest in more robust anti-malware measures, including investments in better firewalls, threat intelligence and enhanced encryption techniques. Cybersecurity firms thus tend to make similar investments in cyber countermeasures in the aftermath of attacks.[25] The firms may also collaborate with each other to address the enhanced threats, further driving similar investment trends across the sector.[26]

Regulatory bodies may also impose new compliance requirements in the wake of a cyber attack. These measures are often aimed at fortifying the sector against future attacks and typically involve the introduction of new cybersecurity standards, protocols and requirements. These regulations are frequently industry-wide, ensuring that companies within the sector adopt similar practices.[27] This homogenization of regulation across the industry further reinforces the similarity in cybersecurity investments and day-to-day operations of cybersecurity firms.

An example of a regulatory response to bolster defense in response to cyber attacks is the New York Department of Financial Services (NYDFS) Cybersecurity Regulation, 23 NYCRR Part 500.[28] This regulation, which came into effect in March 2017, was partially triggered by the increasing severity of state-sponsored cyber attacks targeting financial institutions. The NYDFS Cybersecurity Regulation sets forth stringent requirements for financial services and cybersecurity companies, mandating them to implement robust cybersecurity programs. Among its stipulations, the regulation prescribes the establishment of a comprehensive cybersecurity program which must include a written policy and the designation of a Chief Information Security Officer (CISO). It also requires regular testing and assessment of cybersecurity measures and timely reporting of cybersecurity events to the NYDFS. Additionally, the regulation also demands that where cybersecurity services are outsourced to outside providers, these providers take steps to ensure their client's IT systems and customer information is robustly secured. Cybersecurity defense contractors thus have to invest in meeting these new regulations.

Finally, from an investor's perspective, the increased similarity in cybersecurity investment strategies and regulatory environments creates a perception of cybersecurity defense contractors as a

[18]Akoto (2021).
[19]Lazarovitz (2021).
[20]Marelli (2022).
[21]Willett (2021).
[22]Christen, Gordijn and Loi (2020).
[23]Marelli (2022).
[24]Kutscher (2020).
[25]Kutscher (2020).
[26]Akoto (2021).
[27]Srinivas, Das and Kumar (2019).
[28]New York State Department of Financial Services (2017).

https://doi.org/10.1017/bap.2024.22 Published online by Cambridge University Press

homogeneous group facing similar risks and opportunities. This perception of shared systemic pressures becomes a pivotal driver for investors, who increasingly make investment decisions predicated on sector-wide trends. Additionally, severe cyber attacks tends to increase the scrutiny of cybersecurity defense contractors as a whole. This motivates investors to pay closer attention to sector dynamics rather than just focusing on individual firms. Consequently, investment decisions become more sector-centric. Importantly, investors may expect that heightened cyber threats will lead to increased demand for cybersecurity solutions, thereby boosting the business prospects of these firms. This unified expectation of growth and profitability in the face of rising cyber threats could potentially lead to positive co-movements in the stock returns of cybersecurity defense contractors, indicative of increased market integration for the firms within the sector.[29]

In summary, the severity of state-sponsored cyber attacks can act as a catalyst for a series of interconnected changes that affects the financial health and stability of cybersecurity defense contractors. Firms adopt similar cybersecurity investment strategies and regulators may enforce standardized measures. This incentivizes stock market investors to homogenize their perceptions of the risks and opportunities confronting contractors. Investors thus adopt similar trading strategies in relation to the stocks of cybersecurity defense contractors. This culminates in the increased market integration of contractors, as reflected in co-movement in their stock returns.

Analytical framework

I empirically examine how the severity of state-sponsored cyber attacks affects the stock returns of a sample of cybersecurity defense contractors. Towards this end, I leverage data on cybersecurity defense contractors and state-sponsored cyber attacks over the period 2000 to 2020.[30]

Cybersecurity defense contractors

The analytical sample for this study includes cybersecurity defense contractors that have been at the forefront of serving the United States federal government, military and intelligence agencies. To ensure robustness in the analysis and mitigate temporal biases, only firms that maintained a continuous presence on the stock market from 2000 to 2020 were considered.[31] This 20-year span marks significant milestones in cybersecurity evolution and ensures that the insights derived are grounded in a consistent corporate performance and market participation.

The analytical sample consists of 16 publicly traded firms, capturing the diversity of the U.S. cybersecurity defense industry. A full list of the firms in the sample along with a description of the cybersecurity services they provide is presented in the Appendix. CACI International Inc., for instance, has solidified its reputation by tailoring its cybersecurity services to the nuanced needs of defense and intelligence agencies. Similarly, Cisco Systems offers a blend of networking expertise and cybersecurity innovations for several government agencies.

Beyond niche specialists, the sample includes several traditional defense contractors like General Dynamics, Northrop Grumman, and Lockheed Martin, underscoring the recent symbiotic relationship between traditional defense contracting services and cybersecurity. Their extensive portfolios not only enhance national defense but also fortify cyber infrastructures. The sample also includes legacy tech giants such as IBM, Microsoft, Symantec and Dell Technologies who are also increasingly providing cybersecurity services to military and government agencies. This adds another layer of depth to the sample and illustrates how established tech giants have pivoted and expanded to meet the cybersecurity challenges of national security.

[29]Market integration in this context refers to the degree to which the stocks of firms within a sector move together in response to new information. It's a measure of the efficiency of the market in incorporating information into stock prices (Anand and Cotter 2017).

[30]The sample and time period are both limited by data availability.

[31]This necessarily excludes privately held cybersecurity firms.

https://doi.org/10.1017/bap.2024.22 Published online by Cambridge University Press

This specific focus on American firms stems from the significant role these entities play in the global cybersecurity landscape, particularly in response to state-sponsored cyber attacks. The U.S. defense sector's prominent position in cybersecurity services and their substantial representation in stock markets make them critical subjects for analyzing market reactions to such attacks.

Stock returns and firm data

Data on firms' monthly stock market returns is sourced from the Center for Research in Security Prices (CRSP), a key hub for information concerning financial instruments traded in the United States.[32,33] I aggregate these monthly returns into yearly returns by taking the mean for each year per firm. This approach allows for the mitigation of the impact of short-term market fluctuations and seasonality and offers a more robust representation of each firm's annual performance and overall trend. Furthermore, it allows me to better correlate these returns with yearly data on state-sponsored cyber attacks.

I also obtain a range of data on firm-specific characteristics that offers a broad yet concise accounting of each firm's overall financial health, operational scale and performance. I include this data to account for their potential effects on movements in firms' stock returns. This data is taken from Standard and Poor's Compustat database and includes data on each firm's total assets and liabilities, net income, stockholders' equity and number of employees.[34,35]

The total assets of a firm serve as an important barometer of its scale and economic reach. It encapsulates the firm's resources, including both tangible and intangible assets. On the other side of the balance sheet, total liabilities offer insights into the firm's financial obligations, a critical aspect of assessing its financial stability and risk exposure. Net income captures a firm's profitability, providing a bottom-line view of the its fiscal performance. Stockholders' equity, often referred to as shareholder's equity, provides a measure of a firm's net value and is a critical indicator of a firm's long-term growth potential. Finally, the number of employees is a straightforward yet informative metric that provides insight into the firm's scale of operations. In the appendix, I present descriptive statistics for these variables.

State-sponsored cyber attacks

Data on state-sponsored cyber attacks come from the Dyadic Cyber Incident and Campaign Dataset (DCID) Version 2.0 complied by Maness et al.[36] To construct their dataset, Maness et al. start with a broad internet search of reports of state-sponsored cyber operations and then use reports by government agencies (e.g., Department of Justice indictments, FBI, NSA etc.) and cybersecurity firms (such as FireEye, Crowd Strike and Kaspersky) to confirm attribution. The dataset excludes incidents attributed to non-state actors (such as LulzSec, Anonymous etc.) unless there is strong evidence that they were acting on behalf of the government. They also institute a time lag in the data collection effort to allow for changes in reported attribution of attacks.[37]

The cyber attacks encoded within the DCID dataset span a diverse array of incidents. These range from acts of vandalism and website defacements to more severe offenses like denial of service (DDoS) attacks coordinated through botnets. Furthermore, the dataset records incidents that utilize sophisticated intrusion or infiltration methods. These acts are often marked by their ostensible objective of espionage. These attacks may also aim to disrupt, corrupt or destroy data or computer systems of the targeted entities. My main interest is in examining the effect of cyber attacks on

[32]Center for Research in Security Prices (2023).

[33]The CRSP data is accessed through the Wharton Research Data Services (WRDS) platform (Wharton Research Data Services 2023).

[34]Compustat North America (2023).

[35]Data from Compustat is accessed through the Wharton Research Data Services (WRDS) platform (Wharton Research Data Services 2023).

[36]Maness et al. (2023).

[37]For a comprehensive discussion of the DCID dataset and coding rules, readers can consult Maness et al. (2023).

https://doi.org/10.1017/bap.2024.22 Published online by Cambridge University Press

Table 1. Cyber attacks against the United States

Statistic	N	Mean	Std. Dev.	Min	Pctl(25)	Pctl(75)	Max
Cyber Attacks	18	7.667	5.224	1	4	10	18
Cyber Attack Severity	18	2.983	0.504	2	2.7	3.2	4

co-movement in stock returns of cybersecurity service providers in the United States so I restrict my analysis to state-sponsored cyber attacks aimed at entities within the US.

The DCID dataset provides information on the number of such attacks per year and importantly, the severity of these attacks. The severity scale devised by Maness et al. is numbered 1 through 10, with 1 being the least severe cyber operations (e.g., packet sniffing and probing) and 10 the most severe (e.g., cyber attacks that result in mass casualties). I create two variables based on these indices. The first captures the number of cyber attacks per year and the other captures the mean severity of these attacks per year. Table 1 presents summary statistics relating to cyber attacks against US-based entities. It reports the number of yearly observations on which the values are based, the mean, standard deviation, minimum, 25th and 75th percentile and maximum values.

> One important data limitation to note—the inherently clandestine nature of cyber attacks likely means a sizable proportion of cyber attacks are not captured in the DCID (or any other) dataset because they are either unknown or have not been publicly disclosed. Consequently, to the extent that cyber attacks are under-reported in the DCID dataset, it should bias against finding evidence in support of my hypothesis.

The table presents two metrics, *Cyber Attacks* and *Cyber Attack Severity*. The former, with a mean of approximately 7.67, provides a measure of the average number of cyber attacks aimed at US-based entities per year. The latter sheds light on the average intensity of these attacks, with a mean value of around 2.98.

Firm integration index

A common way to capture co-movement in stock returns among a group of firms is to compute their market integration. As highlighted earlier, market integration refers the extent to which the returns or performance of individual firms mirror the broader movements of the market or a particular sector.[38] A high degree of market integration signifies that the financial dynamics of firms are largely driven by the same underlying factors or trends. In such cases, the fortunes of the firms are closely interlinked and they tend to move in sync with each other. On the other hand, low market integration denotes a degree of autonomy where firm-specific factors, rather than overarching market trends, shape the firm's financial outcomes. This metric provides a quantifiable means of gauging the interdependence of firms within a specific market or sector.

One technique has proven popular for modeling stock return co-movement—Principal Component Analysis (PCA). The PCA helps simplify complexity in high-dimensional data while retaining trends and patterns.[39] It does this by transforming the data into fewer dimensions, termed "principal components." These components are linear combinations of the original variables and are constructed in a manner such that the first principal component explains the most variance in the data, the second principal component explains the second most variance and so on. In essence, PCA provides a road map that helps researchers to identify common underlying dimensions or "components" that explain the maximum variance in the data. In the context of financial market data, these components represent common factors driving stock returns. The degree to which these components explain a particular

[38]Carrieri, Errunza and Hogan (2007).
[39]Billio et al. (2012).

https://doi.org/10.1017/bap.2024.22 Published online by Cambridge University Press

Table 2. Descriptive statistics of US cybersecurity defense contractors' integration levels

Sample	Min	Max	Mean	Med	Std. Dev.	IQR	Skew	Kurt
All Firms	0.00	99.92	62.08	70.74	30.78	49.90	−0.72	2.28

firm's returns can signify its market integration, thus serving as a useful tool to study the interdependence of firms in a given sector.

Following Anand and Cotter,[40] I operationalize a firm's degree of integration within the cybersecurity industry as the proportion of variance in its stock returns that can be explained by the principal components of the collective stock return matrix for all sampled firms. These principal components are conceived as the eigenvectors derived from the return covariance matrix of all sampled firms, embodying common, nationwide factors contributing to the integration levels of firms within the sector. The integration indices of firms lie between 0 and 100, based on the adjusted R^2 from the principal components regression. Higher values indicate higher levels of integration with the US cybersecurity industry while lower values indicate the opposite. That is, firms that are highly integrated will display high dependence on common factors distilled from the aggregated stock return matrix. Conversely, those that are not integrated will display low synchronicity of returns in principal component regressions, signifying their diminished reliance on common industry factors.

I adopt a data-driven, agnostic approach in determining the number of principal components to use. The guiding principle is to capture a sufficient degree of total variance in the data. As such, I use as many principal components as are required to explain 90 percent of the total variance. As a result, the number of principal components varies slightly from year to year. This flexibility in the number of principal components employed each year allows me to effectively capture the evolving temporal dynamics and complexities within the cybersecurity sector.

Table 2 presents a summary of the market integration indices for the sample firms. It reports the minimum, maximum, mean, median, standard deviation, inter-quartile range, skewness and kurtosis for the industry. The mean and median integration index is 62.08 and 70.74 respectively. This indicates that common market factors explain more than half of the variation in the market returns for the industry. The standard deviation and Interquartile range (IQR), which are measures of dispersion, reveal a relatively high variability in market integration across the industry. The skewness score assesses the asymmetry of the probability distribution. The negative skewness suggests the data is right-skewed, an indicator of periodic bursts of high integration in the sector.

On the other hand, the kurtosis score assesses the shape of the distribution. In a normal distribution, the kurtosis is 3 so a kurtosis of less than 2.28 indicates that the distribution has thinner tails and a flatter peak compared to a normal distribution. For my analysis, this means there are fewer extreme values (outliers) than in a normal distribution and firms' integration indices are generally closer to the mean, resulting in a flatter overall distribution curve.

For each firm, I estimate the yearly integration levels over the sample period and use this to construct the median integration of the firms in the industry per year. Figure 1 shows this yearly median variation in integration levels. In the panel on the right, the dashed line is the linear fitted trend while the gray region delineates the 95 percent confidence interval. The plot shows that cybersecurity service providers exhibit growing levels of market integration over time. The panel on the right presents the yearly median integration box plots for the industry. The horizontal line in each box is the median, enclosed by observations from the inter-quartile range (25–75th percentile). The plot shows that the market integration of firms in the cybersecurity industry shows some variation over time.

Table 3 presents the results of linear trend fitting on firms' yearly integration levels. The estimated coefficient is measured by the adjusted R^2 from principal component regressions on individual firms' stock returns. Newey-West standard errors[41] are presented along with t- and p-values. The estimated

[40]Anand and Cotter (2017).
[41]Newey and West (1987).

https://doi.org/10.1017/bap.2024.22 Published online by Cambridge University Press

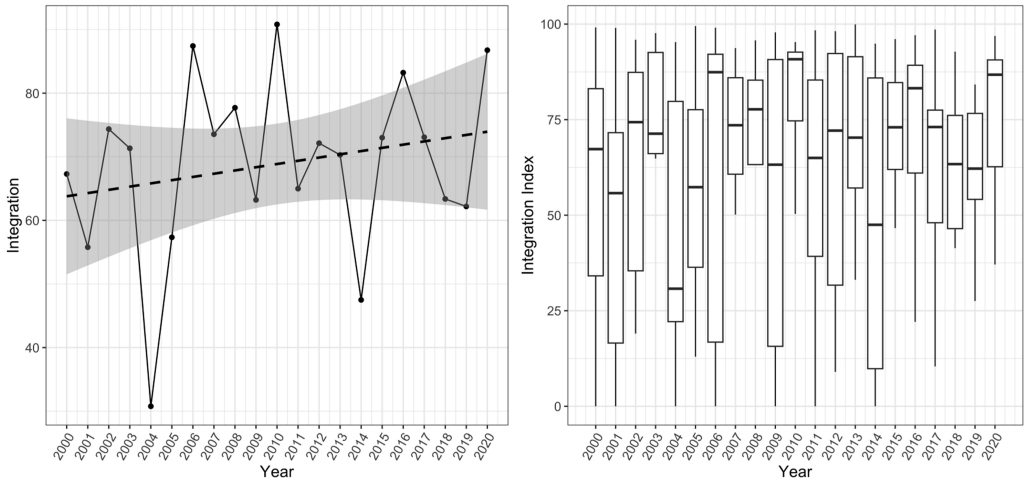

Figure 1. Median integration levels and yearly integration box plots. The panel on the left presents median integration levels for the cybersecurity industry. Integration is measured by the adjusted R^2 from principal component regressions on individual firms' stock returns. The dashed line indicates a linear time trend fitted to yearly integration levels. The gray region is the 95% confidence interval. The panel on the right presents the yearly integration box plots for the industry. Each box plot contains observations from the 25 to 75th percentile, while the horizontal line in each box is the median.

coefficient for the full sample is 0.51, with a *t*-value of 2.52 and a *p*-value of 0.02, implying a statistically significant level of integration across all firms in the cybersecurity industry over the period. This suggests a significant degree of co-movement in firms' stock returns, indicative of common factors impacting firms' returns within the industry.

Figure 2 presents a plot of the cumulative proportion of the variance explained by the Top 10 eigenvectors. The first eigenvector is the solid line at the bottom of the plot and charts how much of the variation in integration levels is explained by the first eigenvector. The second dashed line shows the proportion of variance explained by the first and second eigenvector combined. Similarly, the dotted line at the top of the plot denotes the cumulative proportion of variance explained by all 10 eigenvectors combined.

Figure 3 plots the mean severity of state-sponsored cyber attacks over time. The plot shows that the mean severity of these attacks is steadily increasing over time, underscoring the evolving nature of state-sponsored cyber threats over time. An upward trajectory in attack severity over time implies a potentially increasing strain on the defense mechanisms that cybersecurity contractors must deploy. This heightened severity of cyber attacks not only challenges the resilience of these service providers but also likely influences market perceptions about their efficacy.

Results

I estimate a series of linear models to examine the effect of cyber attack severity on firm market integration. The models include controls for the number of country-level cyber attacks per year, firm-level total assets, liabilities, net income, stockholder's equity and employees. Model 1 has the severity and cyber attack variables, models 2 and 3 progressively include more controls while model 4 has the full complement of control variables. Standard errors for all models are clustered at the firm-level. The results of the analysis are presented in Table 4.

Across all the estimated models, increase in the severity of cyber attacks is positively associated with higher levels of firm market integration. This effect is significant across all the estimated models. This is robust confirmation for our initial intuition—more severe cyber attacks sets in motion a chain of events that culminates in tighter co-movement in the stock returns of cybersecurity defense contractors and a stronger market integration for these firms.

https://doi.org/10.1017/bap.2024.22 Published online by Cambridge University Press

Table 3. US cybersecurity defense contractors' median integration levels

Sample	Estimate	Std. Error	*t*-value	Pr(>|*t*|)
All	0.51	0.20	2.52	0.02

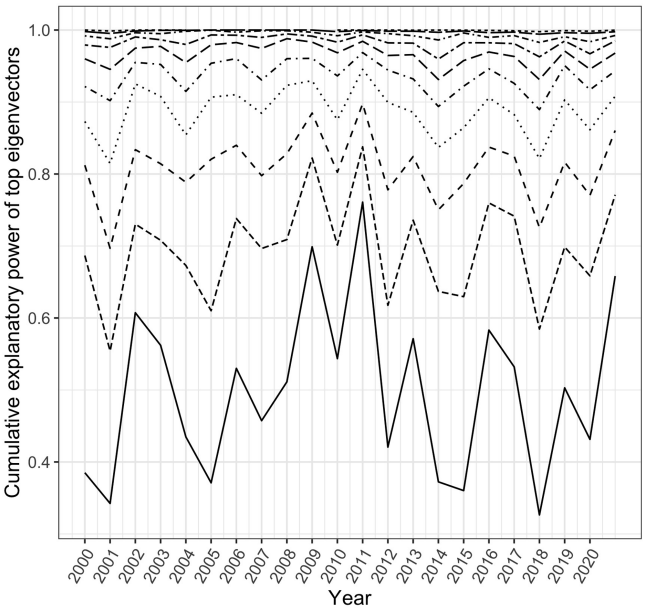

Figure 2. Cumulative proportion of variation explained by the top 10 eigenvectors. The plot shows the cumulative proportion of the variance explained by the Top 10 eigenvectors. The first eigenvector is the solid line at the bottom of the plot and indicates how much of the variation in integration levels is explained by the first eigenvector. The second dashed line shows the proportion of variance explained by the first and second eigenvectors combined. In the same vein, the dotted line at the top denotes the cumulative proportion of variance explained by all 10 eigenvectors combined.

In Figure 4, I illustrate this positive association by plotting increasing values of cyber attack severity against market integration based on the estimated models. In all the plots, there is a clear positive and significant correlation between cyber attack severity and market integration, lending support to the analytical hypothesis. In terms of the control variables, increased frequency of cyber attacks has a negative association to market integration but this effect does not rise to conventional levels of statistical significance. Increase in total assets is has model-dependent mixed effects on market integration while increase in firm liabilities is associated with an increase in market integration, although the significance of these effects are model-dependent. Increases in net income has no significant effect on market integration while an increase in stockholders' equity has a generally small positive effect on market integration. The significance of this effect is also model-dependent. An increase in the size of the firm, as proxied by the number of employees, has a negative effect on the firm's market integration but this effect does not rise to conventional levels of statistical significance.

The appendix has an additional tables that include a fifth model that account for the effect of the involvement of the United States in militarized interstate disputes. Interstate conflict has a positive but insignificant effect on market integration. Overall, the results of the analysis robustly confirm a positive relationship between the severity of state-sponsored cyber attacks and the level of market integration for US-based cybersecurity defense contractors, as evidence by co-movement in their stock returns.

One caveat to note—the focus of the study on American cybersecurity defense contractors means that the results mainly reflect market dynamics specific to the U.S. This may not mirror those in other regions. Markets in Europe, Asia or other parts of the world might react differently to cyber threats due to varying regulatory environments, investor behaviors and economic conditions. Also, different

https://doi.org/10.1017/bap.2024.22 Published online by Cambridge University Press

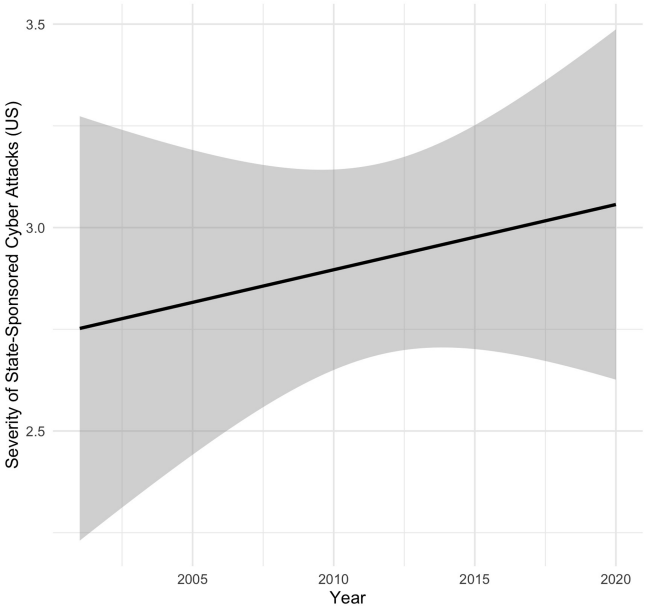

Figure 3. Severity of state-sponsored cyber attacks over time (US). The plot shows the severity of state-sponsored cyber attacks aimed at the United States over time. The mean severity is plotted on the y-axis while the year is on the x-axis. The black line shows the mean trend over time while the shaded region represents the 95 percent confidence interval. The plot shows that the severity of state-sponsored cyber attacks is steadily increasing over time.

countries have varied approaches to cybersecurity, influenced by their unique political, social and technological landscapes. As such, the response of firms in these regions to state-sponsored cyber attacks may not align with the patterns observed in U.S. firms. Moreover, the economic and political contexts in which these U.S. firms operate are distinct. Factors like U.S. government defense spending, foreign policy and international relations can uniquely influence these firms. These factors may thus not be applicable or may have different effects in other countries.

Comparison with cybersecurity firms

An underlying premise of the analysis presented in this paper is that cybersecurity defense contractors are somewhat different from mainstream traditional cybersecurity firms (i.e., firms that primarily offer cybersecurity services aimed at safeguarding information systems, networks and data from unauthorized access). While both are pivotal in safeguarding digital infrastructures, they operate under distinct paradigms that cater to different aspects of cyber defense. This distinction is crucial for understanding their unique roles within the cybersecurity ecosystem.

Recall that cybersecurity defense contractors primarily work with government and defense sectors, focusing on national security interests. Their operations are often aligned with military and intelligence objectives, involving classified projects and national defense strategies. This specialization requires a deep integration with governmental processes, standards and security clearances not typically required of mainstream cybersecurity firms. Also, the solutions provided by cybersecurity defense contractors are often bespoke, tailored to meet the stringent and specific requirements of government and military entities. This contrasts with mainstream cybersecurity firms, which typically offer more generalized cybersecurity services and products designed for a broader market, including private sector businesses and the general public.

These differences means that investor reaction to severe cyber attacks and its subsequent effect on the level of market integration for defense contractors might differ from that of mainstream cybersecurity firms. To examine this, I empirically compare the effect of cyber attack severity for defense contractors and mainstream cybersecurity service providers.

https://doi.org/10.1017/bap.2024.22 Published online by Cambridge University Press

https://doi.org/10.1017/bap.2024.22 Published online by Cambridge University Press

Table 4. Severity of Cyber Attacks and Market Integration

	DV: Market Integration			
	Model 1	Model 2	Model 3	Model 4
Intercept	49.093*** [31.763, 66.422]	52.901*** [32.262, 73.540]	52.404*** [31.844, 72.964]	60.461*** [31.017, 89.904]
Severity	5.089** [0.970, 9.207]	5.393*** [1.358, 9.429]	5.418*** [1.494, 9.343]	5.480** [1.229, 9.730]
Cyber Attacks	−0.468 [−1.499, 0.563]	−0.326 [−1.282, 0.631]	−0.487 [−1.557, 0.583]	−0.676 [−1.895, 0.544]
Assets		0.000 [0.000, 0.000]	−0.001*** [−0.001, 0.000]	0.000 [−0.001, 0.000]
Liabilities		0.000 [0.000, 0.000]	0.000** [0.000, 0.001]	0.000 [0.000, 0.001]
Net Income			0.000 [−0.001, 0.001]	0.000 [−0.001, 0.001]
Stockholders' Equity			0.001** [0.000, 0.001]	0.000 [0.000, 0.001]
Employees				−0.097 [−0.343, 0.149]
Num.Obs.	143	143	143	143
R2	0.024	0.058	0.081	0.091
R2 Adj.	0.010	0.030	0.040	0.044
AIC	1394.5	1393.4	1393.9	1394.3
BIC	1406.3	1411.2	1417.6	1420.9
RMSE	30.84	30.30	29.93	29.76
Std.Errors	by: Firm	by: Firm	by: Firm	by: Firm

Coefficients with 95 percent confidence intervals in parenthesis.*** p less than 0.01, ** p less than 0.05, * p less than 0.1.

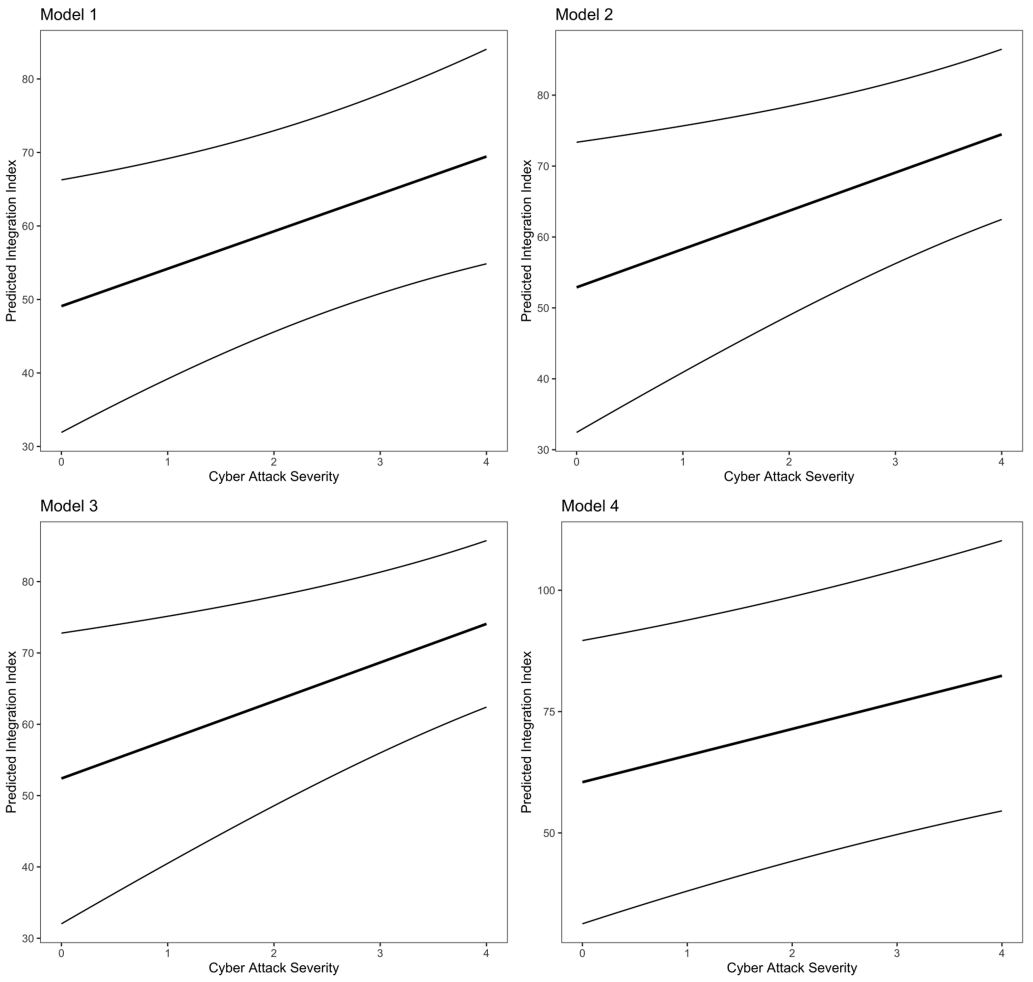

Figure 4. Marginal effect of cyber attack severity on market integration. The plot shows the marginal effect of state-sponsored cyber attack severity on firms' market integration based on the estimated models from Table 4. The dark line is the mean predicted integration level, surrounded by the 95% confidence interval. The plots show increasing market integration given rising severity of cyber attacks.

The sample of mainstream cybersecurity service providers is drawn from the Nasdaq CTA Cybersecurity Index.[42] This index tracks the performance of firms primarily involved in the development, implementation and management of cybersecurity measures for private and public networks. For my analysis, I include companies in the index that are publicly traded on the New York Stock Exchange and leave out any firms already included in our original list of cybersecurity defense contractors. The analytical sample includes firms like CrowdStrike, which specializes in cloud-based services such as advanced threat detection, incident response and cybersecurity advisory and Fortinet, which provides a broad range of cybersecurity solutions including intrusion prevention, anti-virus and endpoint security. It also includes other high-profile cybersecurity firms like Infosys, Zscaler and Check Point. The full list of companies in the sample is included in the appendix.

I repeat the earlier analysis for this sample. The results are presented in Table 5. Across all the estimated models, the coefficient for the severity of cyber attacks is negative but does not rise to conventional levels of statistical significance. This suggests that the severity of cyber attacks does not

[42]Nasdaq (2024).

https://doi.org/10.1017/bap.2024.22 Published online by Cambridge University Press

https://doi.org/10.1017/bap.2024.22 Published online by Cambridge University Press

Table 5. Severity of cyber attacks and market integration (Nasdaq CTA cybersecurity firms)

DV: Market Integration				
	Model 1	Model 2	Model 3	Model 4
Intercept	81.540*** [61.065, 102.014]	82.615*** [62.090, 103.139]	82.145*** [59.667, 104.623]	91.812*** [73.649, 109.974]
Severity	−2.093 [−10.455, 6.269]	−1.398 [−9.919, 7.124]	−1.366 [−10.002, 7.271]	−3.569 [−11.606, 4.468]
Cyber Attacks	−1.031* *[−2.128, 0.066]*	−0.976* *[−2.063, 0.112]*	−0.955* *[−2.027, 0.117]*	−0.771 *[−1.846, 0.304]*
Assets		−0.003*** [−0.005, −0.001]	−0.405 [−1.030, 0.220]	4.460*** [3.353, 5.567]
Liabilities		0.004** [0.000, 0.007]	0.405 [−0.221, 1.031]	−4.459*** [−5.567, −3.351]
Net Income			−0.001 *[−0.009, 0.007]*	−0.001 [−0.010, 0.008]
Stockholders' Equity			0.402 [−0.221, 1.026]	−4.463*** *[−5.568, −3.357]*
Employees				−1.787*** [−2.347, −1.228]
Num.Obs.	111	111	111	110
R^2	0.048	0.133	0.134	0.231
R^2 Adj.	0.031	0.1	0.084	0.179
AIC	1079.2	1072.9	1076.7	1052.4
BIC	1090.1	1089.1	1098.4	1076.7
RMSE	30.16	28.78	28.76	26.65
Std. Errors	By: Firm	By: Firm	By: Firm	By: Firm

Coefficients with 95 percent confidence intervals in parenthesis.
***$p < 0.01$.
**$p < 0.05$.
*$p < 0.1$.

have a clear, significant impact on the level of market integration among this sample of cybersecurity service providers.

The results thus point to a significant difference in investor response between the two groups. For defense contractors, an increase in attack severity unifies investor perception of these firms, leading to closer market integration of the firms' stock returns. In contrast, the severity of cyber attacks does not uniformly influence market behaviors or investor perceptions in relation to mainstream cybersecurity firms to a statistically significant degree.

These differences in investor response could be due to the direct involvement of defense contractors in national security efforts, where increased threats are seen as leading to more substantial governmental, institutional and regulatory action over time. Importantly, investors may view defense contractors as benefiting directly from heightened cyber threats through increased defense spending and contracts, a perception not as strongly applied to mainstream service providers. Moreover, while cybersecurity defense contractors are closely tied to governmental defense mechanisms, mainstream service providers cater to a broader, more varied clientele. This possibly dilutes the immediate financial impact of cyber attack severity on market integration.

Nonetheless, these findings deepen our understanding of how cyber threats differentially impact sectors within the cybersecurity ecosystem. It also emphasizes the need for nuanced strategies to address cybersecurity challenges, tailored to the distinct roles and market expectations surrounding defense contractors and mainstream service providers.

Conclusion

My argument in this paper is that an escalation in the intensity of state-sponsored cyber attacks drives homogenization in cybersecurity investments and the regulatory environment, which in turn causes investors to perceive cybersecurity defense contractors as a group. This perception prompts a behavioral shift among investors, leading to the co-movement of their stock returns. The empirical analysis lends support to this assertion.

As outlined earlier, the results have important implications for the literature. It challenges the commonly held belief that the economic fallout from state-sponsored cyber attacks are isolated to their immediate targets. Instead, the results point towards wider and more systemic cascading effects, highlighting the complex ties between the economy, cybersecurity and national security. Moreover, the results highlight how adversary states, recognizing how intense cyber attacks can affect the stock returns of cybersecurity defense contractors, might strategically exploit this to their benefit. This could open up a new battleground in interstate cyber conflict.

This work is also an important complement to existing studies on the political economy of the cybersecurity industry like Maschmeyer, Deibert and Lindsay[43] who analyze cyber threat reporting by cybersecurity firms. They show that these reports tend to focus on threats to affluent entities capable of purchasing commercial cyber defenses, overlooking threats against entities that cannot afford these premium services. By examining the collective behavior in stock returns of cybersecurity defense contractors following state-sponsored cyber attacks, this study provides insights into how these firms might respond financially to increased threats. The research sheds new light on the underlying commercial motivations that influence strategic decisions within these firms and expands our understanding how cyber threats can propagate through economic channels, potentially influencing a wide array of stakeholders within the cybersecurity ecosystem.

Beyond this, co-movement in stock returns represents an important barometer for the financial health of the cybersecurity industry. This is important because the ability of cybersecurity defense contractors to protect critical computer networks and fend off future attacks could hinge on the collective financial fortitude of the firms in this space. It is thus important to pay close attention to what happens to the returns of these companies as part of a broader effort to ensure national cybersecurity. Limiting the negative impact that market fluctuations have on the stock returns of these companies

[43]Maschmeyer, Deibert and Lindsay (2021).

https://doi.org/10.1017/bap.2024.22 Published online by Cambridge University Press

could be instrumental in the development and innovation of cybersecurity technologies within the sector.

The findings also have important implications for regulatory bodies and policymakers. Given that state-sponsored attacks can catalyze similar corporate investments and compliance requirements, policymakers might consider coordinated strategies that strengthen the sector's resilience. These may include public-private partnerships, incentives for shared threat intelligence and frameworks that encourage diversified investments within the sector.

This research opens up several promising avenues for further exploration. For instance, future studies could investigate the long-term effects of increased market integration in the aftermath of cyber attacks. Are there any ramifications for the cybersecurity defense contracting industry's competitiveness and adaptability? Additionally, research could focus on comparing the responses of cybersecurity markets in geopolitical contexts outside the United States to determine if varying regulatory environments or political tensions play a role in influencing market behaviors post-attack. Also, while this study focuses on the co-movement in stock returns of U.S. defense firms in response to cyber attacks, future studies could consider other potential factors that might influence these market behaviors. For instance, broader economic trends or sector-specific developments might also play a significant role. This broader view would help in understanding the complex interplay of various influences on stock market reactions. In the face of relentless state-sponsored cyber threats, studies that extend the results presented in this study are urgently needed.

Supplementary material. To view supplementary material for this article, please visit https://doi.org/10.1017/bap.2024.28

Acknowledgement. I thank Carlos Felipe Balcázar and participants of the session on Digital Trade, Money, and Cybersecurity at the APSA 2024 Conference for comments and suggestions on earlier iterations of this paper. I also gratefully acknowledge the comments and suggestions of the editors and anonymous reviewers.

Competing interests. The author(s) declare none.

References

Akoto, William. 2021. "Espionage Attempts Like the SolarWinds Hack Are Inevitable, So Its Safer to Focus on Defense Not Retaliation." *The Conversation*.

Akoto, William. 2022. Cyber Economic Espionage: A Framework For Future Research. In A Research Agenda for International Political Economy. (pp. 159–170). Edward Elgar Publishing.

Amir, Eli, Shai Levi and Tsafrir Livne. 2018. "Do Firms Underreport Information on Cyber- Attacks? Evidence From Capital Markets." *Review of Accounting Studies* 23: 1177–1206.

Anand, Abhinav and John Cotter. 2017. "Integration Among US Banks." *Available at SSRN 2932989*.

Attatfa, Amel, Karen Renaud and Stefano De Paoli. 2020. "Cyber Diplomacy: A Systematic Literature Review." *Procedia Computer Science* 176: 60–69.

Baillie, Richard T. and Ramon P. DeGennaro. 1990. "Stock Returns and Volatility." Journal of Financial and Quantitative Analysis 25(2): 203–214.

Billio, Monica, Mila Getmansky, Andrew W Lo and Loriana Pelizzon. 2012. "Econometric Measures of Connectedness and Systemic Risk in the Finance and Insurance Sectors." *Journal of Financial Economics* 104(3): 535–559.

Blinderman, Eric and Myra Din. 2017. "Hidden by Sovereign Shadows: Improving the Domestic Framework for Deterring State-Sponsored Cybercrime." *Vanderbilt Journal of Transnational Law* 50(4): 889–931.

Buchanan, Ben. 2016. *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*. Oxford University Press.

Carrieri, Francesca, Vihang Errunza and Ked Hogan. 2007. "Characterizing World Market Integration Through Time." *Journal of Financial and Quantitative Analysis* 42(4): 915–940.

Cavelty, Myriam Dunn. 2010. Cyber-Security. In The Routledge Handbook of New Security Studies (pp. 154–162). Routledge.

Center for Research in Security Prices. 2023. Online. Center for Research in Security Prices, LLC, An Affiliate of the University of Chicago Booth School of Business.

Christen, Markus, Bert Gordijn and Michele Loi. 2020. *The Ethics of Cybersecurity*. Springer Nature.

Compustat North America. 2023. "Fundamentals Annual." Online. Accessed 01 June 2023. *wrds.wharton.upenn.edu*

Gartzke, Erik and Jon R. Lindsay. 2015. "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace." Security Studies 24(2): 316–348.

Gatzlaff, Kevin M. and Kathleen A. McCullough. 2010. "The Effect of Data Breaches on Shareholder Wealth." Risk Management and Insurance Review 13(1): 61–83.

He, Chris Zhijian, Tracie Frost and Robert E. Pinsker. 2020. "The Impact of Reported Cybersecurity Breaches on Firm Innovation." Journal of Information Systems 34(2): 187–209.

Kamiya, Shinichi, Jun-Koo Kang, Jungmin Kim, Andreas Milidonis and Ren´e M. Stulz. 2018. What is the Impact of Successful Cyberattacks on Target Firms? Technical Report National Bureau of Economic Research.
Kutscher, Jurgen. 2020. "M-Trends 2020: Insights From the Front Lines." Mandiant Threat Research.
Lazarovitz, Lavi. 2021. "Deconstructing the SolarWinds Breach." *Computer Fraud & Security.* 2021(6): 17–19.
Maness, Ryan C., Brandon Valeriano, Kathryn Hedgecock, Jose M. Macias and Benjamin Jensen. 2023. "Expanding the Dyadic Cyber Incident and Campaign (DCID) Dataset: Cyber Conflict from 2000 to 2020." Cyber Defense Review.
Marelli, Massimo. 2022. "The SolarWinds Hack: Lessons for International Humanitarian Organizations." *International Review of the Red Cross* 104(919): 1267–1284.
Maschmeyer, Lennart, Ronald J. Deibert and Jon R. Lindsay. 2021. "A Tale of Two Cybers- How Threat Reporting by Cybersecurity Firms Systematically Underrepresents Threats to Civil Society." *Journal of Information Technology & Politics* 18(1): 1–20.
Nasdaq. 2024. "Nasdaq CTA Cybersecurity Index." Online. Accessed: 4 April 2024.
New York State Department of Financial Services. 2017. "Cybersecurity Requirements for Financial Services Companies." 23 NYCRR 500. on.ny.gov/3r8gz3e
Newey, Whitney K. and Kenneth D. West. 1987. "Hypothesis Testing With Efficient Method of Moments Estimation." International Economic Review pp. 777–787.
Nye, Joseph S. 2014. "The regime complex for managing global cyber activities." *Global Commission on Internet Governance.*
Rid, Thomas and Ben Buchanan. 2015. "Attributing Cyber Attacks." *Journal of Strategic Studies* 38(1-2): 4–37.
Srinivas, Jangirala, Ashok Kumar Das and Neeraj Kumar. 2019. "Government Regulations in Cyber Security: Framework, Standards and Recommendations." *Future Generation Computer Systems* 92: 178–188.
Valeriano, Brandon and Ryan C. Maness. 2014. "The Dynamics of Cyber Conflict Between Rival Antagonists, 2001–11." Journal of Peace Research 51(3): 347–360.
Valeriano, Brandon and Ryan C. Maness. 2015. Cyber War Versus Cyber Realities: Cyber Conflict in the International System. Oxford University Press, USA.
Wharton Research Data Services. 2023. wrds.wharton.upenn.edu. Accessed 01 June 2023.
Willett, Marcus. 2021. "Lessons of the SolarWinds Hack." Survival 63(2): 7–26.

Cite this article: Akoto W (2025). State-sponsored cyber attacks and co-movements in stock market returns: evidence from US cybersecurity defense contractors. *Business and Politics* **27**, 95–113. https://doi.org/10.1017/bap.2024.22

https://doi.org/10.1017/bap.2024.22 Published online by Cambridge University Press