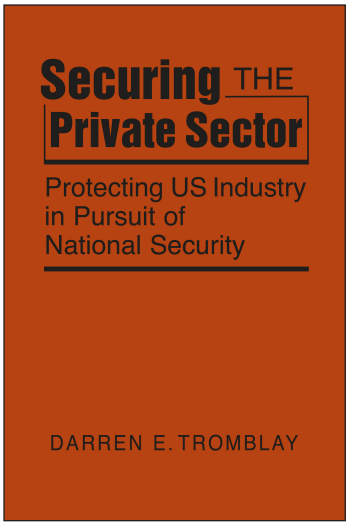
EXCERPTED FROM

Securing the Private Sector: Protecting US Industry in Pursuit of National Security

Darren E. Tromblay

ISBN: 978-1-955055-12-3 hc



LYNNE RIENNER PUBLISHERS

1800 30th Street, Suite 314
Boulder, CO 80301 USA
telephone 303.444.6684
fax 303.444.0824

Contents

1

Private Industry and National Security

THE US GOVERNMENT HAS NEVER BEEN THE SOLE DE FACTO GUARantor of the country's national security. As a concept, national security has continually evolved in its meaning in order to accommodate new geopolitical and technological realities. The private sector plays a significant role in both of these areas by virtue of what it produces, where it does business, and with whom. Through these decisions, the private sector enhances or denies the government's capabilities with which to maintain power.

A particular challenge on which this book focuses is defining the security relationship between the government and elements of the private sector that do not rely on the government for their livelihood. Whereas certain business sectors (e.g., cleared defense contractors) function as extensions of the government and are attuned to national security considerations, many of the most innovative entities, the work of which has significant implications for US national security, do not naturally view their operations in the context of the national interest. This leaves them vulnerable to exploitation or disruption by threat actors, both state and nonstate, who view these entities as soft targets. The challenge for the US government is to bridge the gap in understanding between governmental and industry awareness of threats.

The Private Sector and US Elements of National Power

The flavor of each US National Security Strategy changes with new geopolitical and technological developments. Identification of new threats means that the United States must be able to pivot toward emerging challenges without having to completely retool its approach and develop bespoke solutions to new concerns. It must instead ensure that it has access to the fundamental

tools of geopolitics that it can deploy against new challenges—wherever and from whomever those might emerge. These tools are known as elements of national power and, broadly speaking, consist of diplomacy, information, military, and economics.[1] Ensuring that the US government has access to them allows Washington to address multiple contingencies.

Industry has long been an essential partner in developing elements of national power. For instance, the Lockheed company's "Skunk Works" in Burbank, California, was integral to the development of the U-2 reconnaissance aircraft.[2] The U-2's facilitation of intelligence collection helped to develop the informational advantage of the United States during the Cold War. In this paradigm, industry relies on government patronage and follows its cues on national security. It essentially functions as an extension of the government. However, curation and enhancement of elements of national power are no longer solely the purview of the US government. Many of the capabilities that contribute to elements of national power are increasingly the domain of the private sector.

The relationship between the private sector, the US government, and the acquisition and advancement of capabilities that will support elements of national power has evolved, especially since the end of the Cold War. Increasingly, the private sector innovates and produces new technologies absent government patronage (and therefore absent responsibility to government sponsors). Even in those instances when government has taken a venture capital approach through bodies such as In-Q-Tel and the Defense Innovation Unit, it has been playing catch-up by buying into technologies that are already in development. Furthermore, the private sector is responsible for the bulk of US critical infrastructure, which is essential to elements of national power, particularly economics and information. The mechanisms for ensuring that government and industry find a common understanding of national security, despite responding to different incentives, is the subject of this book.

Dynamics of the Relationship Between the US Government and the Private Sector

Absent its role in directly commissioning technology, the US government and the private sector have developed rules and norms that define their relationship. The most clear-cut regulations are the statutes that define what goods and services industry can provide to whom, and under what conditions transactions can take place. Additionally, there are a number of self-imposed factors, including preservation of market share and ideological pandering, that inform the private sector's willingness, or lack thereof, to work with the US government (even as certain companies test the limits of cooperation with adversarial regimes).

Even though it often acts in its own interests, decoupled from concerns about US national security, the private sector has the ability to develop, or degrade, elements of national power. The field of economics is the element of national power that most people would associate with industry. Thanks to defense contracts, the private sector is also an inextricable participant in developing the military element of national power. Additionally, it is a key player in determining the status of the information element of national power, thanks to its role in developing and deploying means of communication. The ability to instantaneously unleash information on a global scale has been disruptive in both positive and negative ways. It increases "transparency" (although this term has sometimes been hijacked by malignant actors such as WikiLeaks), but also makes deception easier to commit (gullible people consume disinformation and act on it, for example).

Both transparency and deception have real-world implications for US statecraft. They can validate or undercut the narratives that the US government promotes globally. Additionally, private sector facilitation of information flows can strengthen the grip of US adversaries over their countries as well as weaken US allies' ability to support Washington, and, absent gatekeeping, it can allow foreign actors to interfere with US society and politics in a variety of nefarious ways.

Finally, the private sector's decisions have implications for diplomacy through their impacts on the circumstances that US policymakers must navigate. Decisions to sell or not sell certain capabilities to foreign governments change the carrots and sticks that Washington can wield. Furthermore, social media have influenced political outcomes and thereby have the potential to elevate a regime, with which the United States must contend, or unseat an allied government.

Other Vulnerabilities and Profound Consequences

Foreign powers—overtly and clandestinely—can benefit from targets that are not readily linked to, but nevertheless have implications for, elements of US national power. Political scientist Ashley Tellis identified that understanding national power not only is an accounting of visible assets, but also entails unpacking capabilities such as the aptitude for innovation and the quality of the knowledge base.[3] Identifying the linkages between non-obvious targets and elements of national power not only protects the capabilities on which the US government relies, but also helps the private sector to safeguard assets that it might not immediately think of as targets until it is too late to prevent harm to the bottom line.

Consistent with Tellis's assessment, innovation not immediately associated with elements of national power nevertheless has eventual implications

for protecting and promoting them. At the time of this writing, the world was struggling through the Covid-19 pandemic. Health has been a long-standing concern for the United States. The 2010 Department of Homeland Security's *Quadrennial Homeland Security Review* explicitly cited the potential catastrophic impact, equal or greater than deliberate malicious attacks, that a pandemic could cause for the United States.[4] In 2014, the department similarly noted that "a devastating pandemic remains the highest homeland security risk."[5]

Foreign actors have long targeted the ability of the United States to effectively innovate toward solutions to wide-ranging health problems. During the 1940s, the Soviet Union attempted to acquire knowledge that would help the country to mass-produce penicillin, going so far as to approach a US company about purchasing a penicillin plant for erection in the Soviet Union. In the early 1950s, a Soviet agent attempted to gather information regarding details about a new process for synthesizing cortisone out of cheap and abundant raw materials that would enable mass production of the substance.[6] Jump ahead to 2020 and the Russians were still trying to siphon off Western research. The United Kingdom's National Cyber Security Centre announced that hackers, who almost certainly were working on behalf of Russian intelligence, targeted vaccine research in the United States, United Kingdom, and Canada.[7] In July 2020, the US Department of Justice indicted Chinese hackers, working on behalf of China's Ministry of State Security, for targeting Covid-19 research.[8]

The private sector also knowingly provides knowledge to hostile actors. For instance, McKinsey, the global consulting company, has helped China's regime to strengthen its grip over the country.[9] With fewer internal challenges, an authoritarian regime such as China's can focus its efforts outward to challenge the United States, forcing the United States to devote military resources (and by extension economic resources in order to develop effective defense technology) as well as diplomatic resources to countering the China threat.

Harm to the United States via Attacks on the Private Sector

Because the private sector is positioned to influence US elements of national power, it is also a direct, kinetic target of threat actors who are seeking to disrupt the ability of the United States to pursue desired policy outcomes. Attacks—especially sabotage and acts of terrorism—on industry, including private sector–owned infrastructure, have the potential to deny the US government tools it needs to achieve strategic objectives. Informational and economic elements of national power are the most immediate casualties in the case of such attacks. However, by focusing US resources

inward, attacks on critical infrastructure have the potential to distract from diplomatic and military objectives.

Foreign powers (and domestic actors) have historically targeted US infrastructure. Attacks such as the bombing of the Black Tom railroad yard in 1916 by German agents have on occasion been kinetic in nature.[10] More recent threats have had the potential to turn a cyber attack into physical destruction. In 2013, an Iranian hacker obtained unauthorized access to the supervisory control and data acquisition systems of a dam in Rye, New York.[11] Iran and other entities have also historically probed the US electrical grid.[12]

Additionally, foreign actors have threatened to disrupt elements of US national power through activities that have the potential to affect less tangible, but equally essential, functions. For example, in 2016 the United States indicted several Iranian entities associated with the Iranian Revolutionary Guard for attacks on multiple companies in the US financial sector. These attacks disabled websites, prevented customers from accessing accounts, and incurred tens of millions of dollars in remediation costs.[13]

Closing the Loop: A Necessary Relationship

In order to protect its elements of national power, the US government has had—and will continue—to engage in activities directed at securing the private sector from state and nonstate threats. Among the many challenges in this area is the ability to reach a consensus with US industry about what constitutes security and what are industry's responsibilities, both as an entity regulated by the government and as a corporate citizen, in upholding security.

Even if the US government and US companies had a completely congruent understanding of security, which, due to differing incentives, they do not, there would be additional challenges to securing the private sector. Chief among these is the infrastructure for sharing information. Threats are multifaceted, and mitigation of those threats requires a wide range of expertise. Historically, the US government has struggled to address these issues. The challenge has toggled between a single agency being required to handle too many functions (e.g., the National Infrastructure Protection Center of the Federal Bureau of Investigation [FBI]) or too many agencies handling one function (e.g., aspects of cyber-related challenges divided between the FBI and the Department of Homeland Security).

There is not currently, nor has there ever been, an effective mechanism for establishing coherent and meaningful relationships between the government and private sector entities. In the late 1990s, the United States edged toward this by encouraging the creation of an information sharing and analysis center (ISAC), which was supposed to gather, analyze, sanitize, and disseminate private sector information to industry. The National

Infrastructure Protection Center (NIPC) would then disseminate information to the private sector.[14] However, the NIPC's functions were subsequently scattered across government and the ISAC concept became stovepiped, with individual industries each establishing an ISAC. It is time to revisit this concept and develop a clearinghouse for threat information, on foreign entities' intelligence collection and terrorism activities, that has implications for private sector targets. This body would also help to broker relationships between industries and the appropriate government agencies in order to deploy resources—such as the Department of Homeland Security's Cybersecurity Advisers—in furtherance of disrupting threats and mitigating vulnerabilities.

Structure of the Book

This book examines the history and complexity of the relationship between the US government and private industry in seeking to protect industry's contributions to elements of national power. The intent is to develop, through an examination of how these relationships have evolved, a better understanding of how best to engage the private sector in areas of shared security concerns.

Chapter 2 covers the rules of the road for the relationship between government and the private sector. It begins with a discussion of the laws that govern to whom the private sector can provide what, and when the "what" can go to the "whom." Then it specifically addresses the two types of laws—those that govern the "what" (e.g., the Arms Export Control Act) and those that govern the "whom" (e.g., the Trading with the Enemy Act)—that regulate the private sector's relationships with foreign entities. Additionally, it discusses the laws that govern what a foreign entity can and cannot do vis-à-vis aspects of the private sector (i.e., foreign investment and economic espionage). The chapter also provides an in-depth discussion of deemed exports (the transmission of knowledge rather than tangible technology). This will be a continuing problem in an increasingly globalized research and development ecosystem. It is also an area where foreign governments have pushed the boundaries of US laws in order to siphon knowledge through engagement with US companies and experts. Finally, Chapter 2 identifies the informal dynamics of the interaction between government and the private sector (e.g., US government investment, politics, and foreign relations) that complicate the relationship.

Chapter 3 examines the problems of counterintelligence in the private sector. It discusses the long-standing reality that foreign governments directly target the US private sector. (The private sector, because of this vulnerability, also provides a first line of defense for identifying what capabilities foreign governments are attempting to acquire as well as the

methodologies and tactics foreign governments and other threat actors employ.) The chapter discusses the ways in which the US government has countered the threat to the private sector both through coordination across government agencies and by enlisting the American public. It also covers the various initiatives that the government has developed to increase industry's awareness of intelligence threats.

Chapter 4's topic is counterproliferation and counterterrorism. Unlike counterintelligence, both of these functions focus on preventing items from reaching dangerous end-users, rather than on the protection of an informational advantage. Although counterproliferation involves the exfiltration of technology and technological knowledge from the United States, the chapter focuses more on those items that could go boom in the night (or any other time of day). It then addresses how state and nonstate terrorist actors may deploy illicitly acquired technology or knowledge against the US private sector, including critical infrastructure, and discusses the steps taken by the US government to harden private sector targets against attacks from state and nonstate actors. It concludes with how geospatial intelligence (GEOINT) and imagery intelligence (IMINT) could contribute to the protection of critical infrastructure.

Chapter 5 covers the growth of the US government's cybersecurity activities, specifically as they pertain to protecting the private sector. It traces cybersecurity from the foundations that the FBI established, especially in its protection of networks through the National Infrastructure Protection Center, to the Department of Homeland Security's multiple, successive cybersecurity organizations. The reader should view the cyber milieu not as its own threat but rather as an environment that facilitates intelligence and terrorist threat actors.

Chapter 6 tackles some crosscutting considerations created by the changing nature of technology and threat scenarios (i.e., the intersection of actors, implements, and vulnerabilities). The increasingly complex threat environment has prompted the United States to engage in activities beyond its borders in order to protect US interests through the establishment of norms and the collection of information. A skilled, knowledgeable work force is essential to addressing the factors that have made securing the private sector a global challenge. The chapter juxtaposes the ever-expanding challenge with the government's perpetual struggle to hire and retain expertise capable of implementing the government's initiatives vis-à-vis the private sector.

Finally, Chapter 7 revisits the relationship between the public and private sectors. It discusses how government and industry can make common cause around the concept of human security, structure engagement to mitigate the fragmentation of information-sharing, and create opportunities for private sector expertise to inform government.

Notes

1. Congressional Research Service, *Defense Primer: Information Operations* (Washington, DC, 2020), https://crsreports.congress.gov/product/pdf./IF/IF10771.

2. Gregory W. Pedlow and Donald E. Welzenbach, *The CIA and the U-2 Program, 1954–1974* (Langley: Central Intelligence Agency, 1998), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/the-cia-and-the-u-2-program-1954-1974/u2.pdf.

3. Gregory F. Treverton and Seth G. Jones, *Measuring National Power* (Santa Monica: RAND, 2005).

4. Department of Homeland Security, *Quadrennial Homeland Security Review* (Washington, DC, 2010), https://www.dhs.gov/sites/default/files/publications/2010-qhsr-report.pdf.

5. Department of Homeland Security, *Quadrennial Homeland Security Review* (Washington, DC, 2014), https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf.

6. Federal Bureau of Investigation, *Soviet Intelligence Targets in the United States, 1946–1953* (Washington, DC, 1953), https://www.governmentattic.org/2docs/FBI_Monograph_Soviet-Targets-US_1953.pdf.

7. Chris Fox and Leo Kelion, "Coronavirus: Russian Spies Target Covid-19 Vaccine Research," *BBC News,* July 16, 2020, https://www.bbc.com/news/technology-53429506.

8. Department of Justice, "Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information Including COVID-19 Research," https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion.

9. Walt Bogdanich and Michael Forsythe, "How McKinsey Has Helped Raise the Stature of Authoritarian Governments," *New York Times,* December 15, 2018, https://www.nytimes.com/2018/12/15/world/asia/mckinsey-china-russia.html.

10. Federal Bureau of Investigation, "Black Tom 1916 Bombing," https://www.fbi.gov/history/famous-cases/black-tom-1916-bombing.

11. Department of Justice, "Seven Iranians Working for Islamic Revolutionary Guard-Corps Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector," March 24, 2016, https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged.

12. Center for Strategic and International Studies, *Significant Cyber Incidents Since 2006,* https://csis-website-prod.s3.amazonaws.com/s3fs-public/201106_Significant_Cyber_Events_List.pdf.

13. Department of Justice, "Manhattan U.S. Attorney Announces Charges Against Seven Iranians for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector on Behalf of Islamic Revolutionary Guard Corps–Sponsored Entities," March 24, 2016, https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-seven-iranians-conducting-coordinated.

14. Presidential Decision Directive/NSC-63, May 22, 1998, https://fas.org/irp/offdocs/pdd/pdd-63.htm.