# 1

# Introduction

Under what conditions might foreign acquisition of a US company constitute a national security threat to the United States? How should analysts and strategists in the Committee on Foreign Investment in the United States (box 1.1), together with congressional overseers, assess risks and threats to distinguish between the serious and the inconsequential? These are the questions I address in this Policy Analysis.

The potential threats that foreign acquisition of a US company might pose fall into three categories (all of which are of particular, but not exclusive, interest to the functioning of the defense industrial base). The first category ("Threat I") concerns any proposed acquisition that would make the United States dependent on a foreign-controlled supplier of crucial goods or services who might delay, deny, or place conditions on the provision of those goods or services (i.e., the mere fact of dependence does not necessarily warrant a threat designation).

The second category ("Threat II") applies to any proposed acquisition that would allow transfer of technology or other expertise to a foreign-controlled entity (or its government) that might use it in a manner harmful to US national interests.

The "Threat III" designation is for any proposed acquisition that could allow insertion of the means for infiltration, surveillance, or sabotage, whether by a human or nonhuman agent, in goods or services crucial to the functioning of the US economy.

Evaluation of all three threats must consider the relationship between the governments of the two countries involved in a merger or acquisition.

---

*The assessments of all cases in this Policy Analysis are based on the author's independent research of publicly available materials and do not reflect any special knowledge of actual CFIUS deliberations.*

### Box 1.1 The Committee on Foreign Investment in the United States

The Committee on Foreign Investment in the United States (CFIUS) is an interagency committee authorized to review transactions that could result in control of a US business by a foreign corporation or government, in order to determine the effect of such transactions on the national security of the United States. CFIUS operates pursuant to section 721 of the Defense Production Act of 1950, as amended by the Foreign Investment and National Security Act of 2007 (FINSA) (section 721) and as implemented by Executive Order 11858, as amended, and regulations at 31 C.F.R. Part 800.

#### Composition

The secretary of the Treasury chairs CFIUS, and the committee's staff chair, who is the director of the Office of Investment Security in the Department of the Treasury, receives, processes, and coordinates formal case notifications ("notices"). The nine CFIUS members are the heads of the following departments and offices:

- Department of the Treasury (chair)
- Department of Justice
- Department of Homeland Security
- Department of Commerce
- Department of Defense
- Department of State
- Department of Energy
- Office of the US Trade Representative
- Office of Science and Technology Policy

Representatives of the following offices also observe and, as appropriate, participate in CFIUS's activities:

- Office of Management and Budget
- Council of Economic Advisors
- National Security Council
- National Economic Council
- Homeland Security Council

The director of national intelligence and the secretary of labor are nonvoting, ex officio members of CFIUS with roles as defined by statute and regulation.

#### Process

The CFIUS case review process generally begins when parties to a proposed or

*(box continues next page)*

**Box 1.1 The Committee on Foreign Investment in the United States** *(continued)*

pending transaction jointly file a voluntary "notice" with the committee. If the committee finds that the transaction does not present any national security risks or that other provisions of law provide adequate and appropriate authority to address the risks, then CFIUS will so advise the parties. If the committee finds that the transaction presents national security risks and that other provisions of law do not provide adequate authority to address them, then CFIUS may enter into an agreement with or impose conditions on the parties to mitigate such risks or may refer the case to the president for action.

*Source:* US Department of the Treasury, www.treas.gov (accessed on May 26, 2009).

## Analytical Tools for Evaluating the Three Threats

Rigorous identification of the first two types of threats entails similar analytics, so they can usefully be examined together. Evaluation and remediation of Threat III are more complex, as will be apparent in the cases described in chapter 4. Both Threats I and II involve the manipulation of dependence in imperfectly competitive markets. Threat I requires a government to address the potential costs of a foreign acquisition that leaves the economy (and its defense industrial base) faced with a quasi-monopolistic supplier threatening to withhold, delay, or place conditions on the provision of a good or service. The costs of such dependence may be purely economic but may also be political or military.

Threat II involves the opportunity for a foreign government to take advantage of having firms in the position of quasi-monopolistic supplier to other countries—the foreign acquisition might undermine the ability of the firm's home government to wield quasi-monopoly power. As with Threat I cases, the foreign supplier might use such power to extract economic rents and enjoy economic externalities but also to exercise political or military advantage.

Where should CFIUS strategists and congressional watchdogs look for analytical guidance in dealing with Threats I and II? The two most relevant sources of insight are antitrust analysis and strategic trade theory: Threats I and II might be considered special cases of antitrust enforcement, concerned primarily with the conditions under which collusion (defined in this context as a collaboration between the acquiring foreign company and its government rather than between two companies) is most plausible rather than with explicit proof of predatory behavior. Or they might be considered special cases of strategic trade theory, focused on a battle over

the location of externality-rich economic activities but with the goal of not only extracting economic rents but also exercising political and military/strategic advantage.

The most useful features derived from antitrust analysis and strategic trade theory are not the sophisticated and fancy theorizing but rather some simple tools to identify genuine sources of risk and threat (and dismiss bogus claims and allegations).

## Coverage of the Three Threats in Language of CFIUS Legislation

The language of Section 721 of the Defense Production Act of 1950 and of subsequent amendments, including the Foreign Investment and National Security Act (FINSA), includes each of the three types of threats (US Department of the Treasury 2008a). But it fails to provide adequate analytical guidance to distinguish between serious and implausible national security threats.

Concern about Threat I (denial or manipulation of access to supplies) appears in phrasing about whether an acquisition "could result in control of a person engaged in interstate commerce in the United States by a foreign government or an entity controlled by or acting on behalf of a foreign government" (FINSA Section 2, (a), (3) (4)). But nowhere does the Act explain the concept of "control" to mean that the acquirer could delay, deny, or place conditions on the provision of a good or service in a way that might threaten US national security.

Concern about Threat II ("leakage") appears in language about "the potential effects of the transaction on sales of military goods, equipment, or technology."[1] But there is no consideration of whether alternative sources of these items are readily available. Thus, for example, Finmeccanica's acquisition of DRS Technologies (chapter 4) might result in a hypothetical sale of the latter's leading-edge acoustic signal processing system to China (or to a dealer who might transfer it to China), but the availability of commercial off-the-shelf substitutes shows that this Finmeccanica acquisition does not open a channel for "leakage" of unique goods, equipment, or technology.

FINSA addresses Threat III (sabotage and espionage) as follows: "The term 'national security' shall be construed so as to include those issues related to 'homeland security,' including its application to critical infrastructure…. The term 'critical infrastructure' means…systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems or assets would have a debilitating impact on national security" (FINSA Section 2, (a), (5), (6)). For the Bain Capital

1. Section 721 (f) of the Defense Production Act of 1950.

acquisition of 3Com, with Huawei minority ownership (chapter 4), to be fully covered, however, this language would have to be broadened to include infiltration and surveillance, as well as detection of network weaknesses and possible internal system manipulation.

Notwithstanding such gaps, CFIUS members, staff, intelligence community support, and congressional overseers should, in general, be able to find adequate justification in current legislation and regulations to deal with the three types of threats. But they are left without appropriate filters to discern truly troublesome cases from nonthreatening ones. Furthermore, the terms "critical" and "essential" are introduced without qualification, leaving the potential for protectionist mischief. For example, section 2 of FINSA states that "the term 'critical technologies' means critical technology, critical components, or critical technology items essential to national defense" (FINSA Section 2, (a), (7)). According to this definition, foreign acquisition of a US steel producer (as in the Oregon Steel case in chapter 2) would certainly involve an item "critical" and "essential" to national defense, leading the reader to consider such an acquisition a potential national security threat. There is no guidance to point out that the multiplicity of alternative suppliers would render any attempt to delay, deny, or place conditions on supply access entirely noncredible or any transfer of technology inconsequential. This omission is likely to doom debate about foreign acquisitions in the United States (like debate about foreign acquisitions in other countries) to assertions that every "critical" or "essential" sector should be kept in the hands of home-country citizens or businesses.

## Structure of the Analysis

Threat I is the focus of chapter 2, where I explain the criteria necessary to identify a credible likelihood that a good or service can be withheld (or made conditionally available) at great cost to the economy. I draw on historical and contemporary cases, using foreign acquisitions in the semiconductor, steel, and oil industries, to clarify what is "critical" to the United States and consider the potential impacts of manipulation by the home government of a foreign acquirer. (An overview of recent CFIUS acquisition cases, categorized by year, sector, and country, is in appendix A.)

In chapter 3 I analyze Threat II, showing how evaluation of this second type of threat interacts with the analytics of the first. The outcome again depends on the availability of the technological or managerial expertise held by the acquired company and possible gains of the acquisition for the new home government. The chapter uses two classic cases—the proposed acquisition of LTV Corporation's missile business by Thomson-CSF of France and the successful acquisition of IBM's PC business by Lenovo of China—to show the poles of interpretation. Chapter 3 then combines the analytical perspectives required for Threats I and II to examine the highly

controversial case in which the China National Offshore Oil Corporation (CNOOC) attempted to acquire Unocal.

In chapter 4 I discuss Threat III (infiltration and sabotage) in the context of the 2005–06 Dubai Ports World case. In addition, Bain Capital's failed attempt to acquire 3Com, with a minority interest for Huawei of China, provides the opportunity to investigate the interrelationships between Threats I, II, and III, as does Finmeccanica's successful takeover of DRS Technologies.

The analysis concludes with a critical look at analytical tools that might aid CFIUS deliberations (namely, the Herfindahl-Hirschman concentration index as used in antitrust cases and strategic trade theory). Chapter 5 also includes a skeptical discussion of whether Threats I and III can be limited to consideration of consequences for defense industries rather than for the US economy more broadly and of somewhat controversial observations about remediation.