August 2009

89

Policy Analyses in International Economics

THREE THREATS: An Analytical Framework for the CFIUS Process

Theodore H. Moran

PETERSON INSTITUTE
FOR INTERNATIONAL ECONOMICS

THREE THREATS:
An Analytical Framework for the CFIUS Process

THREE THREATS: An Analytical Framework for the CFIUS Process

Theodore H. Moran

PETERSON INSTITUTE FOR INTERNATIONAL ECONOMICS
Washington, DC
July 2009

Theodore H. Moran, nonresident senior fellow, has been associated with the Peterson Institute since 1998. He holds the Marcus Wallenberg Chair at the School of Foreign Service in Georgetown University. He is the founder of the Landegger Program in International Business Diplomacy at the university and serves as director there. In 2007 he was invited to join the Director of National Intelligence Advisory Panel on International Business Practices.

His books include *Harnessing Foreign Direct Investment for Development: Policies for Developed and Developing Countries* (Center for Global Development, 2006), *Does Foreign Direct Investment Promote Development?* (coedited with Magnus Blomstrom and Edward Graham, 2005), *International Political Risk Management: Exploring New Frontiers* (World Bank, 2005), *Beyond Sweatshops: Foreign Direct Investment, Globalization, and Developing Countries* (Brookings Institution, 2002), and *Foreign Investment and Development* (1998).

In 1993–94 he was senior adviser for economics on the Policy Planning Staff of the Department of State. He returned to Georgetown University after the North American Free Trade Agreement and Uruguay Round negotiations. He is a consultant to the United Nations, governments in Asia and Latin America, and international business and financial communities. In 2000 he was appointed counselor to the Multilateral Investment Guarantee Agency of the World Bank Group. In 2002 he was chairman of the Committee on Monitoring International Labor Standards of the National Academy of Sciences.

PETER G. PETERSON INSTITUTE FOR INTERNATIONAL ECONOMICS
1750 Massachusetts Avenue, NW
Washington, DC 20036-1903
(202) 328-9000 FAX: (202) 659-3225
www.piie.com

C. Fred Bergsten, *Director*
Edward A. Tureen, *Director of Publications, Marketing, and Web Development*

Typesetting by Susann Luetjen
Printing by TBD

Printed in the United States of America

11 10 09 5 4 3 2 1

Library of Congress Cataloging-in-Publication Data

Moran, Theodore H., 1943-
Three threats : an analytical framework for the CFIUS process / Theodore Moran.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-88132-429-7
1. Investments, Foreign--United States. 2. National security--United States. 3. Committee on Foreign Investment in the United States. I. Title.
HG4910.M665 2009
332.67'30973--dc22

2009021867

Contents

Preface ix

Acknowledgments xiii

1 Introduction 1
Analytical Tools for Evaluating the Three Threats 3
Coverage of the Three Threats in Language of CFIUS Legislation 4
Structure of the Analysis 5

2 Threat I: Denial of Goods or Services by a Foreign-Controlled Supplier 7
Early Illustrative Cases: 1982–91 8
Critical Is Not Enough: The Case of a Russian Oligarch Acquiring Oregon Steel 11
Analytical Lessons Learned 12

3 Threat II: Leakage of Technology or Expertise to a Foreign-Controlled Entity 15
Proposed Acquisition of LTV Missile Business by Thomson-CSF 15
Lenovo's Acquisition of IBM's PC Business 17
Combining Threats I and II in a Controversial Case: CNOOC's Proposed Acquisition of Unocal 18

4 Threat III: Foreign Acquisitions as a Channel for Infiltration, Surveillance, and Sabotage 23
The Dubai Ports World Controversy 24
Investigating the Interrelationships between the Three Threats 25

5 Implications for CFIUS Strategy: Separating Easy Decisions from Hard Judgments 33
Adapting Antitrust Theory: The Herfindahl-Hirschman Index 34
Strategic Trade Theory 35
The Scope of CFIUS: Defining the Terms 36
Remediation 37

Appendix A: CFIUS Covered Transactions, 2005–07 41
Covered Transactions by Industry Sector 42
Covered Transactions by Country 42
Mitigation Measures 42
Foreign Direct Investment in Critical Technology Industries 43

References 57

Index 59

Tables
A.1 Covered transactions, withdrawals, and presidential decisions, 2005–07 45
A.2 Covered transactions by sector, 2005–07 45
A.3 Covered transactions in the manufacturing sector, 2005–07 46
A.4 Covered transactions in computer and electronics subsector, 2005–07 47
A.5 Covered transactions in professional, scientific, and technical services subsector, 2005–07 48
A.6 Covered transactions by country, 2005–07 49
A.7 Covered transactions by country and sector, 2005–07 51
A.8 Foreign companies most active in acquiring US critical technology firms, 2006–07 53
A.9 US critical technology transactions and deal value by country, 2006–07 54

Figures

A.1 Covered transactions by sector, 2005–07 45
A.2 Covered transactions in the manufacturing sector, 2005–07 46
A.3 Covered transactions in computer and electronics subsector, 2005–07 47
A.4 Covered transactions in professional, scientific, and technical services subsector, 2005–07 48
A.5 Total value of completed US critical technology transactions by country, 2006–07 55

Boxes

1.1 The Committee on Foreign Investment in the United States 2
4.1 Brief description of the Dubai Ports World case 25

Preface

This study adds an important new dimension to the Peterson Institute's long tradition of work on foreign investment in the United States. Our research—matching findings published elsewhere—shows that foreign direct investment among developed countries transfers technologies and management techniques, and generates pressures for competition and imitation, which benefit all countries involved. Paul Krugman and Edward M. Graham were pioneers in showing the contributions of inward investment to the American economy in three editions of *Foreign Direct Investment in the United States*. Gary Clyde Hufbauer, J. Bradford Jensen, and Theodore Moran have works in progress at the Institute that bring these investigations up to date.

But a very small number of individual transactions—foreign acquisitions of US companies—may pose national security risks to the United States. Edward M. Graham and David Marchick analyzed some of the prominent cases and offered suggestions to strengthen the workings of the Committee on Foreign Investment in the United States (CFIUS) in *US National Security and Foreign Direct Investment* (2006). Edwin M. Truman has played a leading role in designing best practices to govern investments by sovereign wealth funds.

Nonresident Senior Fellow Theodore Moran takes these efforts a step further in this Policy Analysis. He provides the analytic tools for separating the small number of cases in which a foreign acquisition might pose a genuine national security risk from the vast number in which no credible threat can arise. Potential threats to national security come in three forms: first, that the proposed acquisition would make the United States dependent upon a foreign-controlled supplier of goods or services

crucial to the functioning of the US economy who might delay deny, or place conditions upon provision of those goods or services; second, that the proposed acquisition would allow transfer of technology or other expertise to a foreign-controlled entity that might be deployed by the entity or its government in a manner harmful to US national interests; and third, that the proposed acquisition would allow insertion of some potential capability for infiltration, surveillance, or sabotage into the provision of goods or services crucial to the functioning of the US economy.

The procedures to distinguish between legitimate and implausible national security concerns that are laid out in this Policy Analysis should prove useful to CFIUS and congressional overseers, as well as to the policy and corporate communities more broadly. In addition, the analytic tools to discern national security risks presented here are carefully designed to be generalizable across all countries, developed and developing; Moran provides a basis for mirror-image policies that could be adopted in Europe, Asia, and across the globe. This study is thus part of a broader effort to allow the benefits of foreign direct investment to continue while authentic dangers are identified and mitigated.

The Peter G. Peterson Institute for International Economics is a private, nonprofit institution for the study and discussion of international economic policy. Its purpose is to analyze important issues in that area and to develop and communicate practical new approaches for dealing with them. The Institute is completely nonpartisan.

The Institute is funded by a highly diversified group of philanthropic foundations, private corporations, and interested individuals. About 35 percent of the Institute's resources in our latest fiscal year were provided by contributors outside the United States, including about 8 percent from Japan.

The Institute's Board of Directors bears overall responsibilities for the Institute and gives general guidance and approval to its research program, including the identification of topics that are likely to become important over the medium run (one to three years) and that should be addressed by the Institute. The director, working closely with the staff and outside Advisory Committee, is responsible for the development of particular projects and makes the final decision to publish an individual study.

The Institute hopes that its studies and other activities will contribute to building a stronger foundation for international economic policy around the world. We invite readers of these publications to let us know how they think we can best accomplish this objective.

C. Fred Bergsten
Director
June 2009

PETER G. PETERSON INSTITUTE FOR INTERNATIONAL ECONOMICS
1750 Massachusetts Avenue, NW, Washington, DC 20036-1903
(202) 328-9000 Fax: (202) 659-3225

C. Fred Bergsten, *Director*

Acknowledgments

I am grateful for comments on earlier drafts from Kenneth W. Dam, Gary Hufbauer, Nicholas Lardy, James Lewis, David M. Marchick, James G. Rickards, Ivan Schlager, Edwin (Ted) Truman, and Dov Zackheim. The errors or omissions that remain are my own. An earlier version of this analysis was prepared under the auspices of the International Business Advisory Panel of the US National Intelligence Council.

THEODORE H. MORAN
June 2009

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.

2

Threat I:

Denial of Goods or Services by a Foreign-Controlled Supplier

Popular debate during the period when the Exon-Florio provision was attached to the Omnibus Trade Act of 1988 vacillated between two poles, a situation that has not changed substantially in the contemporary period. At one extreme is a preference for autarchy—national self-sufficiency—and for maintaining domestic ownership of crucial goods and services and at the other a studied indifference to the nationality of producers and suppliers.

According to the first perspective, a nation should produce internally all goods and services vital to its functioning. The corollary in an age of global ownership is that a nation should preserve ownership of domestic firms that provide crucial goods and services in the hands of its own citizens. This pole of reference is not merely theoretical: Congressional statements regularly express a preference for national self-sufficiency accompanied by full domestic ownership, and independent expert bodies—such as the Defense Science Board—demonstrate grudging reluctance to abandon this ideal (Gansler, forthcoming).

But policies promoting autarchy or self-sufficiency are prohibitively costly. They deny a nation the benefits that derive from international comparative advantage: the gains from lower costs due to different natural endowments, from specialization ("what each nation does best"), and from economies of scale. An autarchic bias holds back dynamic gains from the pressure that comes with international competition to improve productivity and innovate. The desire to keep ownership of crucial sectors in national hands deprives the home economy of the capital, management, and technological edge that foreign owners might bring to local companies. Moreover, the adoption of autarchic policies by any major player in the

international system is likely to provoke similar responses on the part of other nations, with the result that the two countries shut each other off from mutually beneficial interchanges of trade and investment. US interests are therefore best served by designing policies for foreign acquisitions of US companies that the United States would find acceptable if copied by other governments around the world.

According to the second perspective, a nation should rely on whatever combination of economic actors that can perform most efficiently, in the belief that national welfare is maximized with free trade and free flows of investment and technology; the question of foreign ownership of or control over sources of supply should not be allowed to influence market outcomes. This approach limits itself to examining the functioning of markets and the performance of economies without paying attention to the citizenship or national origin of the actors involved.

Over time the debates evolved into a more sophisticated understanding that three criteria are necessary for there to be a credible likelihood that a good or service can be either withheld at great cost to the economy or provided based on unacceptable conditions:

1. the industry must be tightly concentrated,
2. the number of close substitutes limited, and
3. the costs of switching suppliers high.

If suppliers are many in number, are dispersed in location and ownership, and offer easily substitutable goods and services, there is no credible national security threat, no matter how vital the good or service.

Early Illustrative Cases: 1982–91

The case from the 1980s that most effectively illustrated the perils of relying on a foreign-owned supplier emerged from the European experience with the local affiliates of Dresser Industries and General Electric in building the Soviet gas pipeline (Hufbauer and Schott 1985). While neither Dresser nor GE entered Europe via acquisition, the case illustrates the problem of dependence upon sole-source foreign suppliers.

After the Communist declaration of martial law in Poland in 1982, the Reagan administration retaliated against the Soviet Union by issuing a unilateral and retroactive order to the Dresser and GE parents to cancel their contracts to provide high-performance pumping stations for the pipeline. To the consternation of the Europeans, the subsidiaries of these US companies in France and Germany became a vehicle for diktat, causing significant delays and high switching costs for the gas line developers. The French government issued a counterorder directing Dresser's French subsidiary to proceed with the shipment of 21 pipeline booster compres-

sors. In theory, the presence of Dresser facilities on French soil provided tangible assets for the French government to threaten to take over and managers (including American managers) for the French government to threaten to throw in jail. Rather than ensuring compliance, however, a transatlantic corporate stalemate resulted, until US and French authorities broke the impasse at a higher political level. The European governments realized that they were too dependent on the US-owned affiliates, even though the affiliates were operating within European borders (an observation that will be significant in the discussion of "remediation" in chapter 5).

The European experience with Washington directives to Dresser and GE set the scene for US concerns about Japanese acquisitions of American companies during the tumultuous period surrounding the passage of the Exon-Florio provision in 1988. Specifically, there was apprehension that foreign ownership of a firm producing goods or services crucial for the functioning of the US economy, and for which there are no readily accessible substitutes, could create a liability in the event of a political conflict between the host and originating countries.

The Exon-Florio provision arose from a broad concern about the possible decline of US high-tech industries, a concern aggravated by aggressive competition from Japan. In the context of rather shrill rhetoric about "the Japanese threat," however, there emerged an increasingly sophisticated appreciation of what constituted genuine cause for alarm and what did not.

The case that provided the principal impetus for the passage of the Exon-Florio provision was the proposed sale of Fairchild Semiconductor by Schlumberger of France to Fujitsu in 1987. Commerce Secretary Malcolm Baldrige joined Defense Secretary Casper Weinberger in arguing that the sale would give Japan control over a company that served as a major supplier of chips to the US military. Other US semiconductor firms joined the argument against making US defense industries dependent on outsiders for high-tech inputs. Fujitsu withdrew its bid for Fairchild, however, before the completion of analysis to determine whether foreign "control" and "excessive dependence" were valid apprehensions. Shortly thereafter National Semiconductor acquired Fairchild at a substantial discount from the proposed Japanese price, previewing the outcome of the CNOOC-Unocal case (chapter 3). Allegations about threats to national security can become a convenient vehicle for competitors to advance their own takeover plans and have to be evaluated independently and rigorously on the merits.

The battle over Nikon's 1989 proposal to acquire Perkin Elmer's "stepper" division exhibited the kind of careful assessment that the Fairchild Semiconductor case lacked. Steppers are advanced lithography equipment used to imprint circuit patterns on silicon wafers in the semiconductor industry. At the time of the proposed acquisition, Nikon controlled roughly half of the global market for optical lithography and Canon con-

trolled another fifth (Bergsten and Noland 1993, 141). If the acquisition were allowed to proceed, it would have placed quasi-monopoly power in the hands of Nikon (and, by extension, the new owner's home government) and would have significantly constrained the number of sources from which US producers could purchase this semiconductor machinery. Here there was solid justification for a worry that Japanese authorities would acquire the potential to direct the company to delay or deny new products, services, and technologies to US buyers.[1]

The following year debate about Nippon Sanso's proposal to acquire Semi-Gas Systems incorporated a more formal method of evaluation based on concentration of suppliers. The CFIUS process had originally approved the incorporation by Hercules, the US parent company, of Semi-Gas, provider of cabinets that store and distribute the toxic gases used to make chips. But the US Department of Justice pointed out that the acquisition would raise the new Japanese owner's share of the global market to 40 percent and announced therefore that it would lodge an antitrust challenge to the proposed sale. This degree of market concentration raised not just the possibility of monopolistic pricing but also the specter of other forms of sales discrimination. Once again US semiconductor firms, as well as Sematech, the Pentagon-supported industry consortium whose objective was to boost the competitiveness of the US computer chip manufacturing industry, were justifiably wary of finding themselves at the mercy of a foreign supplier of these specialized components.

In 1991 Senator Lloyd Bentsen (D-TX) held hearings at which US semiconductor firms asserted that Japanese firms were disadvantaging US equipment users by withholding or delaying sales of state-of-the-art technology. A US General Accounting Office report (US GAO 1991)[2] did not find convincing support for these assertions or for other illegal or predatory behavior on the part of Japanese suppliers. But the concern about the Japanese government instructing US subsidiaries of home country companies to behave in ways inimical to US national interests was not without foundation—Japan's Ministry of International Trade and Industry, under pressure from Socialist members of the Diet, did force Drexel, the American subsidiary of Kyocera Corporation, to withhold advanced ceramic technology from the US Tomahawk cruise missile program (US House of Representatives 1991, 179).

---

1. The 2000 case of ASML of the Netherlands acquiring Silicon Valley Group to create the world's largest maker of semiconductor lithography equipment posed the same problem. In this case, however, prominent US industry figures—including Craig Barrett, CEO of Intel—lobbied in favor of the acquisition. The dilemma was between dependence on a quasi-monopolistic foreign supplier and reliance on a less capable (and perhaps failing) national producer—a quandary that will resurface in the discussion of "remediation" in chapter 5.

2. Starting on July 7, 2004, the GAO's legal name was changed from General Accounting Office to Government Accountability Office.

Last, experiences during Operations Desert Shield and Desert Storm in 1990–91 illustrate that dependence on foreign suppliers, even for military mission-critical technologies and components, does not necessarily constitute a threat. During these operations, the US Department of Commerce received 91 requests from US companies for assistance in expediting the delivery of products to support US military operations; of particular urgency were parts needed for a radio search and rescue signal that was difficult for Iraq to intercept during a period when Saddam Hussein was trying to capture downed pilots for propaganda value. Five of the required products originated from foreign suppliers (US GAO 1993, 8); the US Department of Commerce contacted the British and Japanese embassies for help. A subsequent GAO investigation found no evidence that foreign companies or governments did not freely cooperate with the United States to expedite the five orders (US GAO 1993).

Critical Is Not Enough: The Case of a Russian Oligarch Acquiring Oregon Steel

"Critical" implies a large negative impact if the economy had to do without the goods and services in question. For CFIUS strategists and congressional overseers, both the likelihood and the impact of having to "do without" cannot be separated from an appraisal of both the availability of close substitutes for those goods and services and the switching costs.

To illustrate the need to balance concern about the "criticality" of a good or service with attention to the degree of concentration among suppliers, I simulate what might justifiably have been CFIUS consideration of the 2006 acquisition of Oregon Steel by the Russian company Evraz, which has close ties to a Russian oligarch, Roman Abramovich, who enjoys friendly relations with the Kremlin.

Could this acquisition pose a national security threat to the United States? Based on the criteria outlined above, for a foreign acquisition to pose a threat that the United States is becoming dangerously dependent on the foreign supplier, CFIUS strategists have to evaluate *both* whether the good or service in question is crucial to the functioning of the country's economy (including but not limited to its military services) *and* whether there is a credible likelihood that the good or service can be withheld (or that the suppliers, or their home governments, could place conditions on provision of the good or service).

The first evaluation clearly raises concerns: Steel is a major component of more than 4,000 kinds of military equipment, from warships, tanks, and artillery to components and subassemblies of myriad defense systems. Uninterrupted access to steel is also crucial for the everyday functioning of the US civilian economy.

But the second evaluation dispels those concerns: In the international steel industry, the top four exporting countries account for no more than 40 percent of global steel trade. Alternative sources of supply are widely dispersed, with ten countries that export more than 10 million metric tons (Belgium-Luxembourg, Brazil, France, Germany, Italy, Japan, Russia, South Korea, Turkey, and Ukraine), and 20 additional suppliers that export more than 5 million metric tons.

Thus although the steel industry remains vital to US national economic and security interests, the multiplicity of sources around the world means that there is no realistic likelihood that an external supplier (or group of suppliers) could withhold steel from, or place conditions on delivery to, US purchasers or the US government. The globalization of steel production allows US users to take advantage of the most efficient and lowest-cost sources of supply without worrying that the United States is becoming "too dependent" on foreigners.[3]

Thus the first guideline prevails: If alternatives are difficult to find, the acquisition might be legitimately objectionable; if alternatives are abundant, the acquisition poses no threat. The second guideline, about the distinction between what is "crucial" and what might be "denied," will appear again in the examination of CNOOC's proposed acquisition of Unocal in the next chapter.

Analytical Lessons Learned

The European experience with Dresser and GE and the US concern about Nikon–Perkin Elmer and Nippon Sanso–Semi-Gas illustrate that a severe concentration among suppliers can give rise to concern about a potential takeover of a US industry or supply whether or not the government where the proposed acquirer is headquartered is an "enemy" (or "hostile").[4] There may be dangers associated with a foreign acquisition even when the home country of the acquirer is normally a friend or ally. The decision to approve, or disapprove, a proposed acquisition by a company from China, India, Russia, or any other nation does not have to be a litmus test for the long-term strategic relationship between that country and the United States.

The "sophistication" that distinguishes this approach from the desire

3. Does this mean that every foreign acquisition in the steel industry should be approved? In 1983 the Department of Defense (DOD) objected to the Japanese purchase of a US specialty steel producer on the grounds that the US firm's output was essential for the production of military aircraft (Jackson 2007, 4). Rather than showing the number of alternative suppliers or estimating the ease or difficulty of switching among suppliers, DOD simply classified the product specifications as secret, rendering analysis by outsiders impossible.

4. The proposed acquisition of the LTV missile division by Thomson-CSF of France (analyzed in chapter 3) illustrates the same proposition.

for self-sufficiency is that dependence on foreign-owned suppliers qualifies as worrisome *only if*, as explained above, the number of suppliers is highly concentrated, substitutes are not readily available, and the switching costs are high (Moran 1990, Tyson 1992). Whether for semiconductor equipment or other crucial inputs to a national economy or its defense industrial base, the crucial criteria are the availability of alternative sources and the ease of shifting from one provider to another. For the threat of delay, denial, or blackmail or the placement of limitations on access or use to be credible, the unavailability of substitutes is the necessary condition.

This analytic tool allows CFIUS strategists to distinguish cases that are legitimately worrisome from those that are not. Many industries will claim that they are "critical" for American economic or military security—and rightly so. But these claimants deserve special attention from CFIUS only if the three criteria are satisfied.

It is important to emphasize that the relevant concentration test is the global market, not the domestic market, and the relevant measurement is whether a proposed acquisition increases the concentration in the global market to a worrisome extent, not whether the acquired firm is the last producer on US soil. Furthermore, whether the target of proposed acquisition is or is not a supplier to the US military is not of analytical importance for Threat I, independent of the number of rival suppliers and the switching costs. A competitive well-diversified foreign supplier base for US defense industries is a source of strength for the US military, not weakness (Gansler, forthcoming).[5]

If the degree of concentration in the industry points to a realistic capability for the home government to manipulate the actions of the newly acquired firm, foreign government ownership may not matter. Thus Dresser Industries became a pawn in the policy struggles between the United States and Europe, and Nikon a pawn in the evolution of the US-Japanese relationship, even though the parent firms were fully privatized. To be sure, independent owners of a fully private company may resist home-country directives with or without success; Dresser Industries, for example, led a fierce fight in Washington to oppose the pipeline policies of the Reagan administration, to no avail.

Is there a precise concentration measure that can be used to separate cases where the possibility of supply manipulation is credible from cases where it is not? In antitrust theory a concentration test helps policymakers judge the empirical likelihood that even the most willing participants will ultimately fail in their efforts to collude successfully. But there is no precise degree of concentration above which more consolidation leads to collusion

5. However, for Threat III—foreign acquisition as a method of infiltration, surveillance, or espionage directed against US government purchasers of goods and services from the acquired company—the issue of whether the military, DOD, or US government agencies are customers is important.

and below which it makes collusion impossible. What is most needed is a straightforward way to dismiss foreign acquisition cases where the risk of delay, denial, or the imposition of conditions is highly unlikely. In chapter 5 I propose that the US Department of Justice/Federal Trade Commission guidelines for mergers and acquisitions offer a useful reference point to guide CFIUS strategy, and (like the similarly structured guidelines of the European Commission Directorate-General for Competition) they are acceptable as the basis for mirror-image strategies on the part of other governments. The guidelines may provide a heuristic separation device, but cases along the margin are almost certainly going to be judgment calls.

3

Threat II:

Leakage of Technology or Expertise to a Foreign-Controlled Entity

A proposed acquisition typically offers the foreign parent corporation some production or managerial expertise that it did not formerly possess, thereby providing the home government of the foreign parent an opportunity to deploy the newfound expertise in ways it deems desirable. Moreover, the additional production or managerial expertise usually strengthens, however marginally, the national defense (and specifically military) capabilities of the new home government.

For assessment of Threat II, the question then is twofold: How broadly available is the additional production or managerial expertise involved, and what difference would the acquisition make for the new home government? The following cases illustrate deliberations to address these questions.

Proposed Acquisition of LTV Missile Business by Thomson-CSF

The prototypical example of potentially worrisome technology transfer is the landmark case of the proposed acquisition of the LTV missile business by Thomson-CSF of France in 1992.[1]

The LTV Corporation found itself in bankruptcy due to underfunded pension obligations associated with the parent company's steel-making

1. Information about this case is drawn from materials prepared by Theodore H. Moran for the Subcommittee on Defense Industry and Technology, Senate Armed Services Committee, April 30, 1992.

operations. To raise cash, a federal bankruptcy court in New York considered proposals from Martin Marietta, Lockheed, and Thomson-CSF of France to purchase LTV's missile division and approved sale to the latter. Some of LTV's missile division capabilities were sufficiently close to those of multiple alternative suppliers that Thomson-CSF could obtain them elsewhere with relative ease. But three product lines—the multiple launch rocket system (MLRS), the Army Tactical Missile System (ATACM) long-range, near all-weather guided missile, and the line-of-sight antitank (LOSAT) missile—had few or no comparable substitutes, and one—the extended range missile interceptor (ERINT)—included highly classified technology that was at least a generation ahead of rival systems and virtually unique at the time. It is not clear from public sources exactly which LTV missile division products and services were formally included in the US export control regime of the time.

Thomson-CSF was 58 percent owned by the French government and had a long history of closely following its directives. Thus concern about the potential for sovereign conflict over the disposition and timing of Thomson-CSF sales, if the LTV missile division became part of the group, was substantial. Previous Thomson-CSF sales to Libya and Iraq had already provoked considerable controversy: A Thomson-built Crotale missile had shot down the sole US plane lost in the 1986 US bombing raid on Tripoli, and Thomson radar had afforded Iraq advance warning in the first Gulf War.

The US Department of Defense initially informed Congress that the Pentagon would insist on a special security agreement, or blind trust, for Thomson-CSF to perform security work on LTV programs, an arrangement that Thomson-CSF first opposed but later accepted. But CFIUS rejected the proposed acquisition when Thomson-CSF and the Pentagon failed to reach agreement on how to ensure that sensitive US technology did not somehow leak to the new French parent. (This concern reemerged in Finmeccanica's proposed acquisition of US defense supplier DRS Technologies; see chapter 4.)

This case demonstrated the importance of establishing a method for determining whether a foreign acquisition might threaten to provide a channel for unacceptable "leakage" of sensitive technology or other know-how. Such a method entails calculating the concentration or dispersion of the particular capabilities possessed by the acquired entity; when the entity presides over unique or very closely guarded capabilities that might be deployed in ways that could damage US national interests, the threat is genuine.

As the treatment of the proposed acquisition of 3Com by Bain Capital, with a minority stake by Huawei Technologies, will illustrate (see chapter 4), potential transfer of technology or know-how to a foreign company, and thence to a foreign government, via acquisition does not mean merely that such technology or know-how might give the latter an edge in capabilities. More importantly, in some circumstances, the acquisition may

enable the foreign government to identify weaknesses, shortcomings, or vulnerabilities to which US purchasers of the company's goods and services, including US government or US military purchasers, are exposed (perhaps unbeknownst to those purchasers). In other words, foreign acquisition might lead the new owner (and its government) to discover a hidden flaw in the company's systems that could be exploited at a later date against those who rely on the systems. Whether the US export control regime (including Department of Commerce Export Administration Regulations and Department of Defense certifications of exemption from Department of State International Traffic in Arms Regulations, or ITAR, categories) is sufficient to identify how the foreign government of an acquired firm might exploit knowledge obtained via the acquisition is not clear; the regulations may catalogue leading edge capabilities that the US government wishes to deny to potential adversaries but not address hidden chinks in the armor of home-country purchasers.

On the other hand, if rivalry among closely matched providers is strong, the potential harmful impact of technology transfer via foreign acquisition is greatly diminished and ultimately vanishes. If the entity that is the object of proposed acquisition presides over capabilities that offer roughly the same performance characteristics as alternative suppliers, the foreign acquisition poses no genuine threat.

Lenovo's Acquisition of IBM's PC Business

Competition among personal computer (PC) producers is sufficiently intense that basic production technology is considered "commoditized"—an observation that informs how CFIUS strategists should look at the Chinese purchase of widely available computer capabilities. More than a dozen producers compete for 50 percent of the PC market, and none shows an edge for long. Enhanced capabilities are embedded in the components, including hardware and software, for general or specialized uses that are sometimes highly concentrated.

An imaginary proposed foreign acquisition of Intel or Cisco would—and should—arouse the most serious CFIUS concerns, whereas an offer to acquire a PC assembler—even by a Chinese or a Russian company with close ties to the home government—should not. It is far-fetched to think that Lenovo's acquisition of IBM's PC business represented a risk of "leakage" of sensitive technology or provided China with military-application or dual-use capabilities that are not readily available elsewhere. (Deciding where the 3Com case falls along this spectrum of concern/nonconcern depends on an analysis of the interrelationship of all three threat types, as discussed in chapter 4.)

Beyond the "leakage" of technology and other capabilities, popular scare stories about foreign acquisitions in the United States sometimes en-

vision foreign investors coming in, like the Soviets in post–World War II Germany, dismantling plants and laboratories, and carting them off. But the reality is otherwise. Data show that foreign investors typically do not even transfer high-value-added activities and leading management functions back to the home country (the so-called headquarters effect) (Graham and Krugman 1989; Graham and Marchick 2006, chapter 3; Marchick and Slaughter 2008). On the contrary, they usually leave the most valuable newly acquired activities and management functions where they are—that is why they bought the assets in the first place—and bring new resources to improve the performance of the existing plants and laboratories.

Thus Lenovo has been expanding its operations in Purchase, New York, near IBM headquarters (in Armonk) and in Raleigh-Durham, North Carolina, even as it absorbed the IBM teams designing and selling ThinkPad notebooks and ThinkCenter desktop computers (IBM had outsourced most of the actual production years earlier). In general, the evidence demonstrates that greater foreign investment in a developed economy, including the US economy, bolsters the capabilities and competitiveness of firms based in the home country (for data see Moran 2009).

Once again, the use of a concentration test to assess Threat II is, as for Threat I cases, likely to be more useful in dismissing implausible assertions of potential harm to national security than in specifying the extent of an extra advantage from possible leakage of technology or product capability. Moreover, evaluations of Threat II will invariably have a dynamic dimension, as a foreign acquisition that affords the new owner (or its government) an initially small advantage may allow them to enhance the acquired capability over time.

Combining Threats I and II in a Controversial Case: CNOOC's Proposed Acquisition of Unocal

Taken together, the measures for identifying genuine national security threats provide the tools for a rigorous analysis of the Chinese oil company CNOOC's proposed acquisition of Unocal. Looking solely at the question of whether oil—and access to it—is "crucial" for the functioning of the US economy and military, the answer is clearly yes. Case closed![2] But from an analytical point of view, the case is far from closed. What about the concentration of alternative suppliers and potential switching costs? What about the potential "leakage" of sensitive technologies and managerial expertise?

2. Press statements on CNOOC's proposed acquisition of Unocal by Representatives Joe Barton (R-TX) and Duncan Hunter (R-CA). See Stephanie I. Cohen, "Lawmakers Rip CNOOC's Unocal Bid," July 13, 2005, available at www.marketwatch.com (accessed on June 17, 2009).

In the year preceding the proposed acquisition (2004) Unocal produced 159,000 barrels of oil per day (70,000 of them in the United States) and 1,510 million cubic feet of gas per day (577 million in the United States)— thus approximately 40 percent of its oil and gas production was in the United States. Unocal had proven reserves of 659 million barrels of oil and 6,658 billion cubic feet of natural gas, of which 26 percent were in the United States.

The proposed acquisition engendered concern that CNOOC might divert some or even all of Unocal's energy supplies exclusively to meet Chinese needs. (Rerouting the production would be a highly complicated and expensive undertaking, however, since US pipelines across western states flow west-to-east; thus oil from the Gulf of Mexico would have to be shipped by tanker via the Panama Canal.) If the Chinese government mandated such a reallocation, it is prudent to suppose that even a privatized CNOOC could be forced to follow home-country directives.

But would this outcome harm the United States? Based on the criteria set forth in chapter 2, such a diversion would constitute a "threat" to US interests (economic, political, or national defense) only if sources of supply are tightly concentrated and switching costs are high. But 21 countries (including 15 non-OPEC countries) have oil for export greater than Unocal's entire US production, and six more could be called on to make up for a large portion of Unocal's US output. With US oil consumption at 20.7 million barrels per day and US oil imports at 12.4 million barrels per day, US buyers would simply replace Unocal's minuscule production (three-tenths of 1 percent of US use) with extra imports, leaving net imports and the US balance of payments in energy unchanged. US courts would force CNOOC to pay the switching costs if contracts were broken.

Although US energy needs would be better served with an energy policy that promotes efficiency, reduces energy consumption, and stimulates the development of new energy sources that do not pollute or contribute to global warming, the idea that CNOOC's acquisition would have affected US national energy interests—negatively or positively—is a mirage. Protection of US interests derives from the dispersed structure and fungible qualities of the international oil industry. Whether CNOOC has Chinese government ownership (as at present) or is someday completely privatized, a CNOOC-Unocal subsidiary could still become the object of conflicting US government or Chinese government directives; however, based on the test of readily available substitutes, such a conflict would not necessarily constitute Threat I.

Could US oil be used to provision the Chinese People's Liberation Army (PLA)? Certainly, if the US government did not legally and/or physically block such shipments. But this would penalize the PLA through supplying more expensive oil from the Gulf of Mexico in comparison to provision from cheaper alternative commercial suppliers nearer to home. (If CFIUS strategists were permitted to enjoy a mischievous sense of hu-

mor, CFIUS would have *required* that a CNOOC-owned Unocal ship all of its North American output back to supply Chinese military forces.)

Moreover, in a bilateral crisis—perhaps over a confrontation across the Taiwan Straits—a CNOOC-owned US-based Unocal actually would represent a hostage in US hands, not the other way around. Allowing Unocal business (and Lenovo-IBM business) to proceed as usual would be a bargaining chip for the US government, helping to offset countervailing Chinese pressures on US investors on the Chinese mainland.

What about the second threat test? Might the sale of Unocal to CNOOC have represented a leakage or loss of technology that could damage the United States? Looking strictly at oil production technology (possible enhancement of Chinese antisubmarine warfare capabilities is considered separately below), the answer is clearly no: If the incorporation of Unocal's technology and managerial expertise into CNOOC enhanced the latter's performance in discovering and producing oil, the result would ease the pressure on world energy markets. That is, the spread of Unocal expertise throughout CNOOC would likely have had a positive global supply effect, even if small. At the margin, if (as is likely) Unocal engineers and managers improved CNOOC performance more than they might improve that of Chevron (the alternative bidder), the result would have been a net benefit for US—and global—energy consumers.

While the Chinese thirst for oil is a challenge that the entire world has to cope with, the Chinese drive to develop new energy sources is part of the solution, not part of the problem. Since the rise in oil prices, global investment in developing-country oil properties has fallen far below what the economics of the market would predict—20 percent below, in the calculations of the International Energy Agency (IEA)—largely due to lengthy haggling between host governments and traditional foreign investors over the extraordinarily lucrative terms involved. The Chinese determination to find additional energy supplies, in contrast, shows a consistent willingness to pay premium prices for properties they can bring into production rapidly. What serves US national interests can be illustrated with a hypothetical question: If the government of China came to the World Bank for loans to support $1 billion of Chinese investments in prospective oil production, would US national interests be served by having the US executive director vote yes or no? The answer is clearly yes, to help ease global production constraints.

But a complete assessment of CNOOC's proposed acquisition of Unocal requires a second pass through the questions of excessive dependence and potential leakage of technology.

The question of excessive dependence arises because the Unocal purchase would have included a wholly owned subsidiary, Molycorp, with the only rare earth mine located in the United States, at Mountain Pass, California (although Molycorp ceased mining production there in 2003, the property remains open on a care-and-maintenance basis). The term

"rare earths" is something of a misnomer, according to the US Geological Survey, as it refers to a "moderately abundant" group of 17 elements—the 15 lanthanides, scandium, and yttrium (Hedrick 2003)—for which there are multiple international sources (the principal exporters are Australia, Brazil, Canada, China, Kenya, Madagascar, Mozambique, and South Africa).[3] In addition, large new rare earth deposits exist in Australia and China (but have not been fully developed because of insufficient demand). Thus CNOOC ownership of Molycorp (via Unocal) would not have appeared to offer the Chinese government tight control over a crucial input for the US economy as substitute supplies are easily accessible.

Some members of the rare earth family, however, are genuinely rare. Europium, for example, is one of the least abundant. It absorbs neutrons and is used in control rods of nuclear reactors. Since the Molycorp property is located in the United States, it is difficult to see how Chinese government directives could have denied the United States access to europium. Nonetheless, it would have been appropriate for a thorough CFIUS analysis to consider whether Molycorp should be included in the proposed CNOOC acquisition of Unocal or sold off to an American buyer.

With regard to potential leakage of sensitive technology, assertions were made that Unocal seismic technology had dual-use possibilities that could not only enhance oil exploration but also reinforce Chinese antisubmarine warfare capabilities. Investigation of these assertions would involve highly specialized—perhaps highly classified—expertise. But the guiding criteria would remain the same: Would the acquisition of Unocal seismic technology confer capabilities that are closely held and not available for Chinese purchase or hire from other alternative sources? The assessment of Threat II hinges on how broadly the technology or managerial expertise conferred is available and what net difference the acquisition would offer to the new home government.

3. Rare earths are used in automotive pollution control catalysts, petroleum cracking catalysts, permanent magnets, rechargeable batteries, fiber optics, and medical applications such as magnetic resonance imaging. All US government stocks of rare earths in the national defense stockpile were sold off in 1998, in consideration of the relative abundance of supplies in the open market.

4

Threat III:

Foreign Acquisitions as a Channel for Infiltration, Surveillance, and Sabotage

Threat III is a separate category of potential threat to US national security in which foreign acquisition may afford the new owner's government a platform for infiltration of the acquired company's operations, clandestine surveillance, or sabotage. Thus, as distinct from Threats I and II, the issue is not whether foreign ownership of a service provider (ports administration) or infrastructure network (telecom) or facility (petrochemical plant) might lead to the denial of services by order of the new owner (or its government) or whether sensitive technology or other management capabilities might be transferred to the new owner (or its government); rather, at issue is whether foreign ownership increases the likelihood that what Edward M. Graham and David Marchick (2006) have called a "fifth column" might be able to penetrate the newly foreign-owned enterprise.

Dealing with Threat III is complicated by the fact that formal responsibility for ensuring the integrity of national infrastructure lies with separate public authorities (e.g., US GAO 2007). In principle this should mean that ownership of the facilities does not matter for CFIUS evaluation, since those public authorities will exercise identical vigilance regardless of the company or nationality of the operator.

In practice, however, the implication for CFIUS strategists is the opposite: Public authorities have to play a deliberately more intensive role in monitoring foreign-owned facilities, and CFIUS strategists must design the process for acquisition approval or rejection in a way that ensures this heightened level of engagement for those authorities. The resulting separate-and-different consideration and possible subsequent separate-and-different treatment (depending on the characterization of

the prospective owner's home country) are fraught with difficult diplomatic and legal problems. Is the United Arab Emirates a particularly close ally whose ownership of US infrastructure or other vulnerable facilities should be welcomed or a potentially unreliable ally whose ownership of US infrastructure or other vulnerable facilities warrants especially careful scrutiny? Should potential ownership of US infrastructure by Taiwanese purchasers be treated the same as a bid from a Canadian company? And does the equivalent or nonequivalent treatment depend on the particular government in power?

In addition to physical infrastructure, a Threat III designation might also apply to foreign ownership of (or participation in) a highly leveraged US financial derivatives firm if such ownership enabled external parties to activate a self-destruct mechanism to generate systemwide market chaos during a political crisis. Indeed, if a meltdown mechanism were cleverly designed the perpetrator(s) could arrange to earn vast sums from the disaster at widely dispersed hard-to-track locations (although they would also have to calculate their losses from harm inflicted on the global economy).

Besides rejection of a proposed acquisition, CFIUS may deal with Threat III via remediation of the kind used for foreign takeovers involving classified technologies and materials, by, for example, requiring separate compartmentalized divisions that require US citizenship and special security vetting.

The Dubai Ports World Controversy

The Dubai Ports World case (described in box 4.1) in 2005 raised this third concern. Prior to initial CFIUS approval, the Department of Homeland Security (DHS) negotiated a "letter of assurance" with Dubai Ports World, stipulating that the company would operate all US facilities with US management, designate a Dubai Ports World corporate officer to serve as point of contact with DHS on all security matters, provide information to DHS whenever requested, and assist other US law enforcement agencies on any matters related to port security, including disclosing information requested by US agencies (Graham and Marchick 2006, 138).

It is not clear how much "comfort" such assurances are likely to provide, however, in highly politicized acquisition cases where US authorities are convinced a dedicated threat potential exists. They were not particularly effective in the Dubai Ports World acquisition case. As Senator Frank Lautenberg (D-NJ) commented, "Don't let them tell you this is just the transfer of title. Baloney. We wouldn't transfer title to the Devil; we're not going to transfer title to Dubai!" (Graham and Marchick 2006, 136).

Box 4.1 Brief description of the Dubai Ports World case

In October 2005 Dubai Ports World, a firm that manages container terminals and other port-related operations in 14 countries and is based in the United Arab Emirates, sought to acquire the Peninsular and Oriental Steam Navigation Company (P&O), a British firm, for $6.8 billion. P&O's main assets were terminal facilities owned or leased in various ports around the world, including facilities at six US ports—in Baltimore, Houston, Miami, New Orleans, Newark, and Philadelphia.

The members of CFIUS approved the sale in November 2005 and it was set to close in March 2006. They regarded the transaction as sufficiently routine that they briefed neither political officials nor Congress. However, another company, Eller, which was battling convoluted civil litigation in London against P&O, alerted several congressmen in early 2006, and by February full-throated opposition erupted on Capitol Hill. President Bush and his cabinet members tried to quell the protest without success.

Three charges were leveled against the Dubai Ports World takeover: first, that Dubai had served as an organizational locale for some of the terrorists involved in the attacks of September 11, 2001; second, that Dubai Ports World is largely owned by the government of Dubai, and specifically the emir; and third, that, as a matter of principle, neither US port facilities nor other "critical infrastructure" should be owned by foreign persons, public or private.[1] Faced with overwhelming opposition in Congress, including an adverse 62 to 2 vote in the House Appropriations Committee, Dubai Ports World conceded on March 9, 2006, stating that it would sell the US port facilities acquired from P&O to a US-controlled firm.

Source: Hufbauer, Wong, and Sheth (2006, chapter 5).

1. In fact, many US port and airport facilities as well as other establishments that might be deemed "critical infrastructure" are already owned or controlled by foreign firms—some, such as Citgo, with government participation. This information was not widely known to Congress or the public before the Dubai Ports World case.

Investigating the Interrelationships between the Three Threats

Proposed Acquisition of 3Com by Bain Capital

In late 2007 Bain Capital, headquartered in Boston, proposed to acquire 3Com, a leading US hardware and software network company based nearby, for $2.2 billion, with 16.5 percent minority shareholding by Huawei

Technologies of China, including the right to appoint three of 11 board members (US Securities and Exchange Commission 2008). Huawei was founded in 1988 by a former Chinese army officer, Ren Zhengfei. The Rand Corporation (Medeiros et al. 2005) reports that Huawei maintains close ties with the Chinese government, in particular the People's Liberation Army (PLA). The Department of Defense *2008 Annual Report to Congress on the Military Power of the People's Republic of China* identifies Huawei, along with Datang and Zhongxing, as working closely with the PLA on techniques of cyber warfare.

3Com had already formed a joint venture with Huawei in China, referred to as H3C, which the 3Com parent subsequently bought out to incorporate into its production chain as a wholly owned affiliate. For its part, Huawei has larger market penetration in Europe than in the United States and could make use of a stake in 3Com to provide channels into the US market independent of any interest in 3Com products or services.

How might this acquisition have posed a national security risk to the United States? The case provides insight into the interaction among the different types of threats.

The list of 3Com products suggests that there are as many as nine clusters of goods and services—security solutions (in particular, TippingPoint), convergence/IP telephony, LAN switches, modular switches, stackable/edge switches, LAN transceivers/cables, network interface cards, network management, and routers—that might be considered crucial to the functioning of the US economy (and the US defense industrial base) and that might provide important capabilities to the Chinese economy (and defense industrial base). These nine clusters are therefore appropriate for testing against the Threat I criteria of concentration and switching costs.

Looking at denial of access (also Threat I), could the Bain purchase, with the Huawei minority stake, lead to circumstances (perhaps during a US-China crisis) in which critical 3Com capabilities were withheld from US users? On its face, it would appear implausible that a minority interest acquired by Huawei would be enough to allow Chinese interests—or, ultimately, the Chinese government—to dictate how 3Com goods and services were offered for sale on the market. Although a large fraction of 3Com products are assembled in the wholly owned H3C affiliate and shipped from China, and thus could be embargoed by the Chinese government during a foreign policy standoff or military confrontation, the proposed Huawei ownership share in 3Com would not enhance the options available to the Chinese government.

Turning to Threat II, could the Bain purchase, with the Huawei minority stake, allow the "leakage" of sensitive technology or other capabilities to Chinese users that they would not otherwise have access to? CFIUS threat assessment would need to discern for each of the nine clusters whether alternative suppliers were few enough—and switching costs high enough—that the acquisition offered a nonreproducible channel to

obtain the technology or other capabilities. A survey of public sources indicates that most of the routers, switches, and Internet card capabilities of 3Com products are rather widely available commercially and that many involve hardware and software already produced in China.

Particular focus, however, was on 3Com's integrated security and intrusion-protection system TippingPoint, which features US government and military agencies among its purchasers. The 3Com TippingPoint system is built around an application-specific integrated circuit (ASIC)-based engine that performs thousands of high-speed checks on each data packet the recipient receives. How concentrated is the international market for this kind of threat suppression engine? A review of commercial sources suggests that there are at least 12 US players in this market (Cisco Systems, Juniper Networks, Sourcefire, IBM, McAfee, Top Layer Networks, Radware, NFR Security, Reflex Security, DeepNines, StillSecure, and NitroSecurity) as well as European and Asian firms. Specialized expertise would be required to compare the individual attributes of these security systems, but it appears that Chinese agencies have access to capabilities similar to those of TippingPoint. Nonetheless, after some initial reluctance, 3Com and Bain announced that they were prepared to spin off the TippingPoint operations.

Reports of CFIUS objections continued, however, suggesting that concerns extended beyond potential leakage of technology.[1] The public also weighed in. Internet discussions among engineers, technicians, and self-proclaimed experts entertained (or rejected) various formulations of Threat III—that the Bain/Huawei acquisition of 3Com might allow the insertion of some capability for infiltration, surveillance, or sabotage into goods or services crucial to the functioning of the US economy and defense industrial base.[2] There was also concern that the proposed acquisition might provide insight into a system's weak points that even purchasers and users (including those in the US government and defense industrial base) might not be aware of. Once again the most obvious candidate for such security abuses was TippingPoint, where a Huawei ownership stake (and three Huawei board members) might enable the Chinese to identify vulnerabilities to penetration to which the US government, military, and other buyers would be unwittingly exposed. However, this does not appear to be the sole concern, since 3Com and Bain reported that CFIUS objections persisted even after they announced willingness to divest TippingPoint.

---

1. In addition, the *Washington Times* leaked news that CFIUS had serious national security concerns about the proposed acquisition, provoking criticism about violations of confidentiality on CFIUS submissions. See Bill Gertz, "Intelligence Report Hits China Deal," *Washington Times,* November 30, 2007, A-1.

2. "Is 3Com Selling Out the U.S. to Chinese Spies?" Reactions to blog posted by Heidi N. Moore on the Wall Street Journal's WSJ Blog, Deal Journal, March 4, 2008, http://blogs.wsj.com/deals (accessed on June 17, 2009).

By process of elimination, the principal remaining apprehension must have been that a Huawei ownership stake and board members might enable the Chinese to engage in espionage or sabotage of US infrastructure via 3Com routers, network interface cards, or switches. On this topic, Internet assertions of engineers, employees, and former employees of 3Com, Huawei, H3C, and other companies in the same sector both supported and dismissed Threat III risks.[3] Some pointed out that 3Com Ethernet routers and switches are standards-based and already produced and widely used in China.[4] Others argued that it is universally assumed that the manufacturer of a particular system has special modes of entering or manipulating its own systems. One self-identified former Huawei engineer, now in the United States, described how highly trained teams at Huawei R&D centers in Shenzhen and Shanghai dissect US products and then provide reports of how they operate and where their weaknesses or vulnerabilities lie to the PLA and China's National Security Bureau. Pooh-poohing this revelation, technicians from various US firms responded that all companies have "competitor analysis" teams that test and perform reverse engineering on others' products to identify flaws as well as strengths. Adding spice, one engineer asserted that the Department of Defense/National Security Agency routinely inserts "backdoors" and "trapdoors" into key components sold by Cisco and others in China.

The question of whether partial acquisition of 3Com might offer points of intrusion and/or insights into system weaknesses that the Chinese would not otherwise be able to acquire will remain unanswered. Bain announced on March 19, 2008, that it was withdrawing the proposal to acquire 3Com. In the aftermath, bloggers remained divided between those who thought the acquisition posed a real national security threat and those who considered the uproar a combination of anti-Chinese hysteria and behind-the-scenes commercial maneuvering by Cisco and other US competitors to prevent Huawei from gaining a well-established network for commercial sales in the US market.

Finmeccanica's Proposed Acquisition of DRS Technologies in 2008

Finmeccanica is an Italian industrial group operating globally in the aerospace, defense, and security sectors and is one of the world's leading groups in helicopters and defense electronics. It is the European leader in satellite and space services as well as in its know-how and production capacity in energy and transportation. The Italian government has 33 percent ownership and the right to appoint half of the board members. Head-

3. Ibid.

4. "3Com Vaults to #1 in China for Enterprise Stackable Switches and Routers," press release, April 9, 2008, available at www.3Com.com (accessed on June 16, 2009).

quartered in Rome, with a large industrial base in the United Kingdom as well as important production facilities in the rest of Europe and the United States, Finmeccanica has nearly 70,000 employees (including 2,000 in the United States, where it is a supplier to the Department of Defense), and had revenues of more than €13 billion in 2007.

DRS Technologies is a leading supplier of integrated products, services, and support to military forces, intelligence agencies, and prime contractors worldwide. Its products are deployed on a wide range of high-profile military platforms as well as on other platforms for military and nonmilitary applications.

In May 2008 Finmeccanica signed a merger agreement under which it proposed to acquire 100 percent of DRS stock for $81 per share in cash. The proposed transaction allows Finmeccanica to consolidate its international role as a major supplier of integrated systems for defense and security and to enter the US market as a key player; it allows DRS to seek new business opportunities in the United States and abroad.

Complexities surrounding the proposed acquisition emerged as soon as Finmeccanica discovered that DRS was engaged in several large special access programs (SAPs)—programs so secret that even knowledge of their existence required an exceptionally high level of compartmentalized security clearance. In addition, the Finmeccanica case raises national security concerns that span all three threat categories. The company's Italian government ownership stake exposes the provision of goods or services needed by the US military to possible political objections, depending on the government in power in Rome (Threat I). Even more worrisome are Threat II concerns along the lines of the LTV–Thomson-CSF case: that the proposed acquisition could allow the Finmeccanica parent to transfer DRS technology or other expertise to a foreign buyer who might deploy it in a manner harmful to US national interests.

Probably less likely is the direct form of Threat III—that the Finmeccanica parent might insert some mechanism for surveillance or sabotage into DRS products—although the acquisition might allow the Italian parent to understand flaws or weaknesses in the performance of DRS products and services, an understanding that could be transferred to others.

The key to determining whether the acquisition might pose a threat to US national security lies in the answers to the following questions:

- Can the Finmeccanica parent company or its Italian government board members interfere with DRS Technologies contracts to supply the US military (Threat I)?
- Are DRS goods and services that are not widely available in commercial markets classified and subject to US export controls (Threat II)?
- Do mitigation arrangements effectively prevent leakage of goods and

services to the Finmeccanica parent that are not widely available in commercial markets, are classified, and are subject to US export control (Threat II)?

- Do mitigation arrangements keep the Finmeccanica parent from gaining insight into (and possibly exploiting) potential flaws and weaknesses in DRS goods and services that would otherwise be shielded from external scrutiny (Threat III)?

A brief assessment of some DRS products sheds some light on the answers to these questions. For example, DRS sells receiver control software (RCS), which is a collection of Windows applications for real-time control and monitoring of various DRS receivers. This software is subject to US export controls, so Finmeccanica could not disseminate it without approval from the US government. On the other hand, DRS produces a specialized system for target acquisition/designation that is not classified or subject to export controls, so presumably Finmeccanica could disseminate it to foreign buyers without securing US government approval or violating the special security agreement (SSA). Similarly, DRS produces an acoustic signal processing system that, although used by the US Navy for underwater surveillance, is listed as a commercial off-the-shelf (COTS) system. So again Finmeccanica could sell this system to, say, China or North Korea (or to a dealer who might transfer it to them) without problem, because these countries could acquire the capabilities on the open market.

The SAPs are classified and presumably subject to export controls, but it is impossible, by definition, for outside observers to know even what kinds of goods and services might be involved.[5] Finmeccanica has a representative on the SSA board and thus participates in board discussions; it also has access to management and can promote synergies with Finmeccanica platforms and systems. The Finmeccanica directors have a fiduciary duty to protect the company's economic interest while the board's government security committee protects national security and ensures that Finmeccanica does not have inappropriate access to classified information.[6] As in the LTV–Thomson-CSF proposal, Finmeccanica offered to set up an SSA isolating it from access to classified information.

To acquire DRS Technologies, CFIUS required Finmeccanica to set up two separate US subsidiaries. The first operates under an SSA for operations up to and including a security classification of "secret." The SSA has three "outside" directors who are unaffiliated US citizens appointed by the Department of Defense and two "inside" directors appointed by

5. Indeed, most CFIUS principals and staff, congressional counterparts, and lawyers and financial participants in a transaction such as this do not have clearances that allow them access to this highly compartmentalized information.

6. Under an SSA, unlike a proxy agreement, the foreign investor is not passive.

Finmeccanica (one Italian, the other a US citizen). In addition, because the Finmeccanica parent is precluded from access to classified information, there is a special security monitor office: Visits by Finmeccanica personnel to the subsidiary have to be approved by the board; all calls from Finmeccanica personnel have to be logged in; and electronic communication with Finmeccanica must be monitored. The second subsidiary, called a "proxy" subsidiary, also has three US citizens appointed by the Department of Defense as directors who serve as proxies for Finmeccanica directors. The proxy subsidiary oversees all contracts (including SAP contracts) classified as "top secret" and above. The Finmeccanica parent is limited to an annual meeting with the proxy subsidiary board and management to review financial issues associated with subsidiary operations. Each of the two subsidiaries is expected to be financially viable on its own. The CFIUS mitigation process included tough negotiations about what and how much nonclassified DRS business would go into which subsidiary.

On October 22, 2008, Finmeccanica announced that it had received all required US regulatory approvals to proceed with the acquisition of DRS Technologies.

5

Implications for CFIUS Strategy:

Separating Easy Decisions from Hard Judgments

In this Policy Analysis, I have presented some simple guidelines for CFIUS strategists and congressional overseers to determine when a proposed foreign acquisition might pose a threat to US national interests and when it would not.

For the three possible types of threats analyzed, a thorough assessment requires first determining the criticality of the goods or services provided by the target of the proposed acquisition—that is, what the costs would be if provision were denied or manipulated, or how much advantage the foreign purchaser and its government would gain through the acquisition of specialized knowledge or technology, or how extensive the damage would be from surveillance or disruption in the acquired company or network. This analysis of "criticality" must be combined in each case with a second assessment to determine the availability of alternative suppliers and the ease of switching from one to another. The objective of this second investigation is to calculate the probability that a foreign-controlled supplier of goods or services crucial to the functioning of the US economy might delay, deny, or place conditions on access to them (Threat I), or that a foreign-controlled entity (or its government) might deploy acquired technology or other expertise that was not otherwise available in a manner harmful to US national interests (Threat II), or that a foreign-controlled supplier of goods or services crucial to the functioning of the US economy might use them for infiltration, surveillance, or sabotage (Threat III).

How accurately can this probability be estimated? Are there standards to guide CFIUS decision making? The most obvious recourse is to turn to

the long-standing guidelines on mergers and acquisitions from the US Department of Justice/Federal Trade Commission (US DOJ/FTC 2006) or the similar European Commission Directorate-General for Competition (European Commission 2008). Drawing on oligopoly theory, these guidelines indicate the level of concentration necessary to create a plausible likelihood that the acquiring company can successfully exploit the transaction to unfair advantage (by restricting production, raising prices, or engaging in some other manipulation of the market) (Levenstein and Suslow 2006).

Adapting Antitrust Theory: The Herfindahl-Hirschman Index

The starting point for the DOJ/FTC guidelines is the concentration ratio in the industry—say, three firms controlling 60 percent of the market—but a simple concentration ratio ignores how large in size and abundant in number the remaining firms in the industry are. The standard correction for this defect is the Herfindahl-Hirschman Index (HHI), which is the sum of the squares of the market shares of all market participants. The HHI shows how far the market concentration deviates from an industry in which all firms are of equal size, an outcome with the least chance of successful collusion. The HHI takes into account the relative size and distribution of the firms in a market and approaches zero when a market consists of a large number of firms of relatively equal size. The HHI increases both as the number of firms in the market decreases and as the disparity in size between those firms increases. Under both US and EU law, in markets with an HHI below 1000 concentration is considered low, between 1000 and 1800 moderate, and above 1800 high.

The next step is to consider how a proposed acquisition will affect the concentration of the industry. Cases that merit DOJ/FTC scrutiny are those in which the postacquisition HHI falls between 1000 and 1800 and the change in the HHI is less than 100 or the postacquisition HHI is above 1800 and the change in the HHI is less than 50. These break points are widely accepted as a guide to public policy; for foreign acquisition cases, they could quite reasonably become the basis of US CFIUS policy as well as for mirror-image legislation in other countries.

But CFIUS strategists and congressional overseers should not be misled about the precision that this use of the HHI will afford. Actual cases vary considerably in the world of antitrust (US DOJ/FTC 2006, 22), and the same should probably be expected in foreign acquisitions. The principal use of the HHI will likely be to dismiss cases where market control and manipulation are highly implausible (a useful accomplishment) but cases along the margin will continue to be judgment calls.

Strategic Trade Theory

In addition to antitrust theory, another source of inspiration for policy toward foreign acquisitions is strategic trade theory, which also treats the manipulation of dependence in imperfectly competitive markets. Strategic trade theory moves beyond monopolistic pricing to the capture of rents and then to the battle over location of externality-rich kinds of economic activity (Brander and Spencer 1981, Krugman 1986).

The preoccupation with Threat I, after all, derives from the concern not merely that a foreign acquirer might withhold provision of a key military input but that another nation might use foreign acquisitions as part of a broader strategy (including trade protection and government subsidy) to gain domination in individual industries, an accusation that was made against Japan in the 1980s (Tyson 1992).

Along the same lines, a Threat II designation may mask an intention to block foreign acquisitions as a way of preserving the quasi-monopoly position of domestic firms, while consolidating the location of spillover-laden research and production activities on home-country soil. The next logical step might be from preventing "leakage" of capabilities that provide military advantage to outsiders to stopping "leakage" of those that generate externalities for the home economy and extract rents from others.

But designing policies to capture externalities and rents is notoriously tricky. It requires not only detailed hard-to-get information but also highly uncertain judgments made by public and private managers under very dynamic circumstances—a feat with unexpected outcomes even in highly stylized single-industry simulations (e.g., Boeing vs. Airbus). The effort to design a strategic trade policy is highly prone, moreover, to political capture: If Boeing becomes a designated US national champion, why not Pfizer, or Caterpillar, or US Steel?

Even if a strategic trade policy (including protection from foreign acquisition) could be formulated and executed perfectly, it is not at all clear that having domestic firms maintain control over their own assets means that those assets will be deployed only on home-country soil or benefit only home-country workers and communities.

Finally, explicit strategic trade policies adopted by one country would doubtless be copied by others, leading to a race of interventions (including trade protections and selective public subsidies as well as shields against foreign ownership) designed to grab rents and externalities at the expense of others.

Again, this depiction is not a straw man or the idle musing of academics. Strategic trade aspirations (or something resembling them) regularly appear in discussions of the defense industrial base as well as in congressional commentary (US DOD 2005–07).

It is probably wise therefore to deal with Threat II in what might be

called a defensive (rather than offensive) mode, preventing leakage of some capability that might be deployed to the detriment of the United States rather than attempting to maintain national ownership of *any* capability that might generate externalities or oligopoly rents.

The Scope of CFIUS: Defining the Terms

Does the preceding analysis suggest that CFIUS strategists and congressional overseers should, as the CFIUS mandate states, limit themselves in identifying the risks a foreign acquisition might pose to "national security" rather than to "economic security"? Much rhetorical energy has been expended arguing over which term—"national security" or "economic security"—should constitute the grounds for CFIUS evaluation, without much rigor in identifying what threat(s) are covered by either.[1] Instead, the debate has been largely tactical, led by those who want to limit the CFIUS mandate to "national security" in order to preclude US government agencies and congressional watchdogs from using the committee as a protectionist device whenever disruption of workers, firms, or communities might result from a foreign takeover.

Safeguarding CFIUS outcomes from protectionist political instincts is a worthy goal. But from a rigorous analytic perspective, a close look at the nature of the risks considered here shows that, however "national security" and "economic security" might be defined, the CFIUS mandate cannot be limited to what affects defense industries or the military, at least for Threats I and III. With regard to Threat II, if the United States were to forswear all efforts to gain national advantage by promoting and manipulating control over tightly concentrated industries, as recommended above, CFIUS deliberations would be limited to preventing leakage of capabilities with military or defense industrial applications (although these could include extensive dual-use capabilities).

Threat I, however, has always been harder to limit to purely military or defense industrial activities. The risks associated with dependence on a foreign quasi-monopolistic supplier (as illustrated by the proposed Japanese takeover of the US maker of semiconductor lithography "steppers"; chapter 2) expose the United States to potential external manipulation that could damage the civilian economy as well as the defense industrial base. It is something of a stretch—but not, alas, an impossibility—to imagine foreign acquisition of a US company with capabilities crucial to the functioning of the economy for which alternative suppliers are extremely few (if available at all) such that the home government of a new owner might delay, deny, or place conditions on the provision of those capabilities with an impact not limited to military or defense industrial users. Hypothetical

1. For background on this debate, see Graham and Marchick (2006, 172–73).

examples might include Chinese acquisition of Intel, Indian acquisition of Cisco, or a Gazprom acquisition of Exxon-Mobil.

Threat III extends quite explicitly from the military/defense arena into the civilian realm. Whatever the particular merits of the 3Com case, the risk requiring CFIUS investigation was whether foreign ownership might afford an opportunity to conduct espionage or to sabotage a network with broad-based usage throughout the economy. The CFIUS test is not solely whether the foreign acquisition would expose military or defense industrial users to potential harm but whether the acquired company's products might provide entrée that could endanger all who rely on the information technology network, the utility network, or the financial network.

If analytic rigor demands that "national security" be defined broadly enough to include the potential for broad disruption and manipulation of the US economy, should the CFIUS legislation be rewritten to reflect this? The answer is almost surely no, unless all of the strictures about industry concentration and switching costs were also spelled out to reduce the potential for using the broader definition for simple protectionist purposes. But if such strictures could adequately be reflected in CFIUS legislation, this accomplishment could then serve as the basis for international harmonization of investment regulation (beginning with the European Union), similar to the broad thrust of competition policy.

Remediation

The preceding analysis also inspires difficult rethinking about the tenets of remediation.

Does the requirement that a US firm acquired by a foreign owner maintain production facilities on US soil ensure access to the goods and services produced by the newly acquired company? The evidence from the Soviet gas pipeline case suggests wariness about assuming an affirmative answer. As noted in chapter 2, when Dresser Industries established a subsidiary in France, French authorities accepted at face value its vow to obey all French laws and mandates. They did not anticipate the ensuing transatlantic corporate stalemate that required political intervention between the US and French authorities to break the impasse.

The directive from Japanese authorities to Drexel, the US subsidiary of Kyocera Corporation, to refuse to supply specialized ceramics for use in the US Tomahawk cruise missile did not generate a counterdirective from the US Department of Defense. But if it had, Kyocera Corporation would have been caught, like Dresser, between conflicting sovereign mandates.

If a proposed acquisition exposes the US economy (or the US defense industrial base) to being at the mercy of a quasi-monopolistic supplier, should the acquisition always be blocked? Often one company will consider acquiring another (or will seek to be acquired) because the company

to be acquired is suffering in the marketplace and needs an infusion of cash or technology to survive and prosper. Silicon Valley Group found itself in such straits when ASML of the Netherlands proposed a takeover in 2000. The dilemma, as Intel CEO Craig Barrett pointed out in urging CFIUS to approve the acquisition, is that US buyers (including defense industrial buyers) might have to make do with less effective goods and services if the US producer is left on its own or is forced to accept an offer from a less accomplished American suitor.

Can sensitive or classified technologies and processes in a firm that is the target of foreign acquisition be adequately protected via a special security arrangement or a blind trust? There is very little public-source research or reporting on this topic. Available data, however, suggest that US government oversight may be rather tenuous since information on the (six) principal protective measures collected by the Defense Security Service of the US Department of Defense comes from self-reporting on the part of the companies (US GAO 2005).

Finally, how should the CFIUS process deal with acquisition-related potential threats that evolve over time? Prior to Alcatel's acquisition of Lucent Technologies in 2006, a CFIUS review was considered final unless it turned out that the parties had provided CFIUS authorities with materially incomplete or false information, whereupon a review could be reopened. Since Lucent owned Bell Labs, which creates classified communication and surveillance technologies for the US Department of Defense, Alcatel was required to create a separate US subsidiary—headed by former US Secretary of Defense William Perry, former CIA director James Woolsey, and former National Security Agency chief Kenneth Minihan—that would handle all classified contracts. But this security compartmentalization did not provide a legal safe haven for Alcatel. Instead the US government reserved the right to reopen the CFIUS review at some later point and to impose new conditions or even require the nullification of the transaction. Using what have come to be called "evergreen" reservations, CFIUS may have given its deliberations in this case the bureaucratic equivalent of eternal life. It is unlikely that American multinationals will find these "evergreen" provisions very appealing when they begin to appear elsewhere in the world.

Appendix A

CFIUS Covered Transactions, 2005–07

In 2005–07, companies filed 313 notices of transactions with the Committee on Foreign Investment in the United States (CFIUS). The number of these transactions—all covered under Section 721(m)(2) of the Defense Production Act of 1950, as amended by the Foreign Investment and National Security Act of 2007 (FINSA, PL 11-49)—rose from 64 in 2005 to 111 in 2006 and 138 in 2007 (table A.1). In 2005, one filing resulted in an investigation (but was withdrawn before completion of the investigation). In 2006, 14 notices were withdrawn during the review and 7 resulted in investigations (although only 2 saw them to completion).

In 2007, 10 notices (approximately 7 percent of the total of 138) were withdrawn during the CFIUS review. Six led to a 45-day CFIUS investigation, of which five were withdrawn during the period of investigation (US Department of the Treasury 2008b, section I). In three of the five investigations, the parties provided a new notification and CFIUS concluded the review without objection within the next 30-day review period. In two of the five investigations, the parties abandoned the transaction. In the one outstanding investigation, changes in the structure of the transaction meant that the foreign company no longer gained control of the US entity, with a consequent determination that the transaction was not covered under Section 721. The president did not take action to suspend or prohibit any foreign acquisition in 2007. During this three-year period, there were two presidential decisions, in each case not to suspend or prohibit the transaction.

This appendix draws from US Department of the Treasury (2008b).

Covered Transactions by Industry Sector

Almost half of the notices filed with CFIUS in 2005–07 involved US businesses in the manufacturing sector (148, or 47 percent), which includes computer and electronics companies, and more than one-third were in the information industry (112, or 36 percent), which includes publishing and telecommunication companies. Table A.2 and figure A.1 provide a breakdown by sector and year. Of the notices that involved the manufacturing sector, computer and electronic products accounted for 34 percent and transportation equipment another 20 percent (table A.3 and figure A.2). The trend in the manufacturing sector has been declining, however, from 53 percent of the total in 2005 to 48 percent in 2006 and 44 percent in 2007 (table A.2).

Of the 51 notices in the computer and electronic products subsector, 41 percent involved semiconductor and other electronic components (table A.4 and figure A.3). Navigational, measuring, electromedical, and control instruments accounted for another 25 percent of all notices. In the professional, scientific, and technical services subsector of the information sector, 40 percent of the notices involved architectural, engineering, and related services (table A.5 and figure A.4).

Covered Transactions by Country

Investors from Canada, France, and the United Kingdom accounted for 44 percent of the 313 notices filed with CFIUS in 2005–07 (the United Kingdom alone, with 79 notices, accounted for 25 percent of the total) (table A.6).

CFIUS reported to Congress that there did not appear to be any clear tendency of companies in one country to prefer transactions in a specific industry sector (table A.7) (US Department of the Treasury 2008b, 11). Rather, countries typically offered up multiple notices among different sectors.

Mitigation Measures

Since CFIUS first negotiated a "mitigation measure" in 1997 to apply to a covered transaction, CFIUS agencies have entered into 52 mitigation agreements. The committee reports that these mitigation measures include a number of different types of legally binding undertakings, ranging from national security agreements (NSAs), which CFIUS describes as contracts to address specific risks, to letters of assurance, which CFIUS describes as simpler documents covering less complex cases (US Department of the Treasury 2008b, 15–16). For mitigation measures adopted since FINSA

became effective, the Treasury Department appoints a lead agency or agencies to monitor compliance and report back to the committee. CFIUS requests that signatory agencies to mitigation entered into before FINSA became effective report on compliance with those mitigation measures.

CFIUS negotiated 6 mitigation agreements in 2005 and 15 in 2006, and in 2007 signed 14 mitigation agreements related to 12 separate transactions (two of which had two agreements).

Four US agencies serve as government parties to the 2007 agreements. Seven of the 14 agreements had just one CFIUS member agency as the US government party; the other seven had two or more.

The 14 mitigation agreements involve transactions in basic manufacturing, energy, operations services for the aviation and maritime industries, and information technology (both hardware and software). Eleven of the agreements constitute letters of assurance to a US government agency or agencies, outlining actions the parties agreed to take to address the national security concerns raised by CFIUS (US Department of the Treasury 2008b, 15). Three of the agreements were NSAs, of which two were new and one was an amendment to an existing NSA.

CFIUS reports that US government agencies monitor compliance by the companies via a number of methods that include periodic reporting to the agencies by the companies, on-site compliance reviews by the agencies, third-party audits (when provided for by the terms of the mitigation agreement), and investigations and remedial actions if anomalies or breaches are discovered (US Department of the Treasury 2008b, 16).

Foreign Direct Investment in Critical Technology Industries

According to FINSA, "The term 'critical technologies' means critical technology, critical components, or critical technology items essential to national defense." The technologies covered are identified in the Military Critical Technologies List, which CFIUS describes as a compendium of existing goods and technologies that the Department of Defense assesses would permit significant advances in the development, production, and use of military technologies by potential adversaries (US Department of the Treasury 2008b, 24). CFIUS reports that this list was augmented with input provided by the White House Office of Science and Technology Policy.

The critical technologies are grouped in 14 sectors, with North American Industry Classification System (NAICS) or Standard Industrial Classification (SIC) codes assigned to each. The sectors are advanced materials and processing, chemicals, advanced manufacturing, information technology, telecommunications, microelectronics, semiconductor fabrication equipment, military-related electronics, biotechnology, professional and

scientific instruments, aerospace and surface transportation, energy, space systems, and marine systems.

As of the end of 2006, 23 percent of the stock of total foreign direct investment was in sectors that include critical technologies, up from 19 percent in 1997 (US Department of the Treasury 2008b, 30). The share of value added by foreign-owned firms in sectors that include critical technologies rose slightly from 22 percent of all value added by all foreign-owned US firms in 1997 to 23 percent in 2005. The share of employment by foreign-owned firms in industries that include critical technology sectors rose from 19 percent of all employment by US affiliates of foreign firms in 1997 to 21 percent in 2005.

Twenty-two foreign companies completed four or more acquisitions involving US critical technology firms in 2006–07 (table A.8). Only four of the companies on this list were also listed as most active in 1993–2005: Thomson Corporation of Canada had 10 mergers with or acquisitions of US critical technology companies during the recent period, compared with 18 earlier; Siemens AG of Germany had 8 mergers or acquisitions in 2006–07, compared with 15 during the previous period; Nokia of Finland had 7 during the recent period, compared with 15 earlier; and Koninklijke Philips of the Netherlands had 4, compared with 14 during the earlier period. CFIUS pointed out, however, that if the parent listed the acquirer as a subsidiary with a different name from that of the parent company the relationship would not be picked up (US Department of the Treasury 2008b, 32).

The 1,073 proposed or completed foreign mergers with or acquisitions of US critical technology companies in 2006–07 examined by the US Department of the Treasury (2008) involved acquirers from 57 countries. Of those 57 countries, 51 countries' investors *completed* 869 transactions. The M&A activity was dominated by investors from five countries: United Kingdom, Canada, Japan, Germany, and France. Together with India, acquisitions by investors from the six countries accounted for 569 of the 869 completed mergers with or acquisitions of US critical technology companies, or 65 percent of the total.

Germany, United Kingdom, France, and Japan were the four largest foreign acquiring countries of US critical technology companies in terms of value. As shown in table A.9, although the United Kingdom was the home country to the acquirers of the most US critical technology companies by number, German acquirers ranked first in terms of value. Canada ranked eighth in value, but second in terms of number of deals. The discrepancy between deal numbers and deal value by country reflects the difference in the reported values of the transactions. Figure A.5 provides the breakdown of reported deal value by country.

Table A.1 Covered transactions, withdrawals, and presidential decisions, 2005–07

Category	2005	2006	2007	Total
Number of notices	64	111	138	313
Notices withdrawn during review	1	14	10	25
Number of investigations	1	7	6	14
Notices withdrawn during investigation	1	5	5	11
Presidential decisions	0	2	0	2

Table A.2 Covered transactions by sector, 2005–07 (percent of total in parentheses)

Sector	2005	2006	2007	Total
Information	24 (38)	32 (29)	56 (41)	112 (36)
Manufacturing	34 (53)	53 (48)	61 (44)	148 (47)
Mining, utilities, and construction	1 (2)	15 (14)	11 (8)	27 (9)
Other		1 (1)		1 (<1)
Wholesale trade	5 (8)	10 (9)	10 (7)	25 (8)
Total	64	111	138	313

Figure A.1 Covered transactions by sector, 2005–07 (percent)

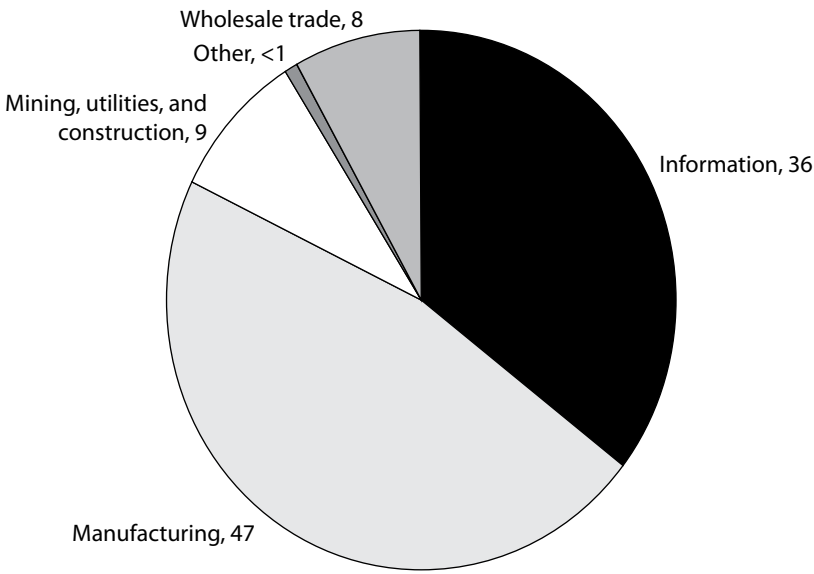


Table A.3 Covered transactions in the manufacturing sector, 2005–07

Manufacturing subsector	NAICS code	Number of notices	Percent of total manufacturing
Textile product mills	314	1	1
Petroleum and coal products	324	4	3
Chemical	325	12	8
Plastics and rubber products	326	5	3
Nonmetallic mineral products	327	3	2
Primary metal	331	7	5
Fabricated metal products	332	5	3
Machinery	333	16	11
Computer and electronic products	334	51	34
Electrical equipment, appliances, and computers	335	9	6
Transportation equipment	336	30	20
Miscellaneous	339	5	4
Total		148	100

NAICS = North American Industry Classification System

Figure A.2 Covered transactions in the manufacturing sector, 2005–07
(percent of total manufacturing)

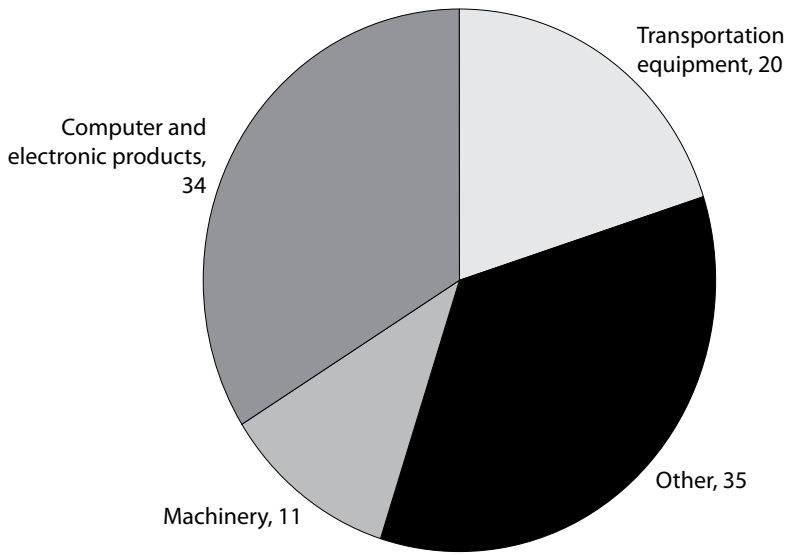


Table A.4 Covered transactions in computer and electronics subsector, 2005–07

Category	NAICS code	Number of notices	Percent of total notices
Computer and peripheral equipment manufacturing	3341	8	16
Communications equipment manufacturing	3342	9	18
Semiconductor and other electronic component manufacturing	3344	21	41
Navigational, measuring, electromedical, and control instruments manufacturing	3345	13	25
Total		51	100

NAICS = North American Industry Classification System

Figure A.3 Covered transactions in computer and electronics subsector, 2005–07 (percent of total in subsector)

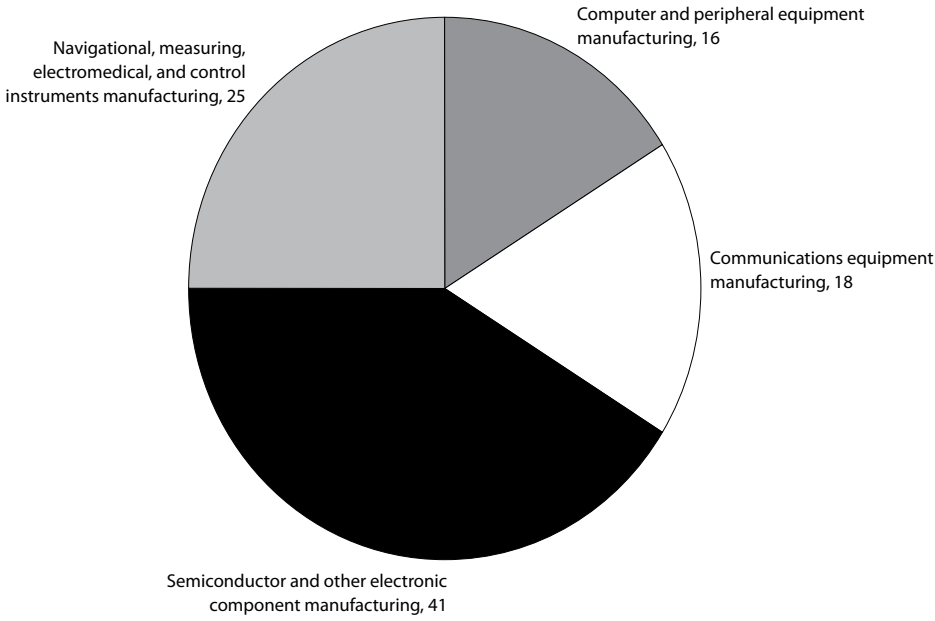


Table A.5 Covered transactions in professional, scientific, and technical services subsector, 2005–07

Category	NAICS code	Number of notices	Percent of total notices
Architectural, engineering, and related services	5413	21	40
Computer systems design and related services	5415	21	40
Management, scientific, and technical consulting services	5416	7	14
Scientific research and development services	5417	3	6
Total		52	100

NAICS = North American Industry Classification System

Figure A.4 Covered transactions in professional, scientific, and technical services subsector, 2005–07
(percent of total in subsector)

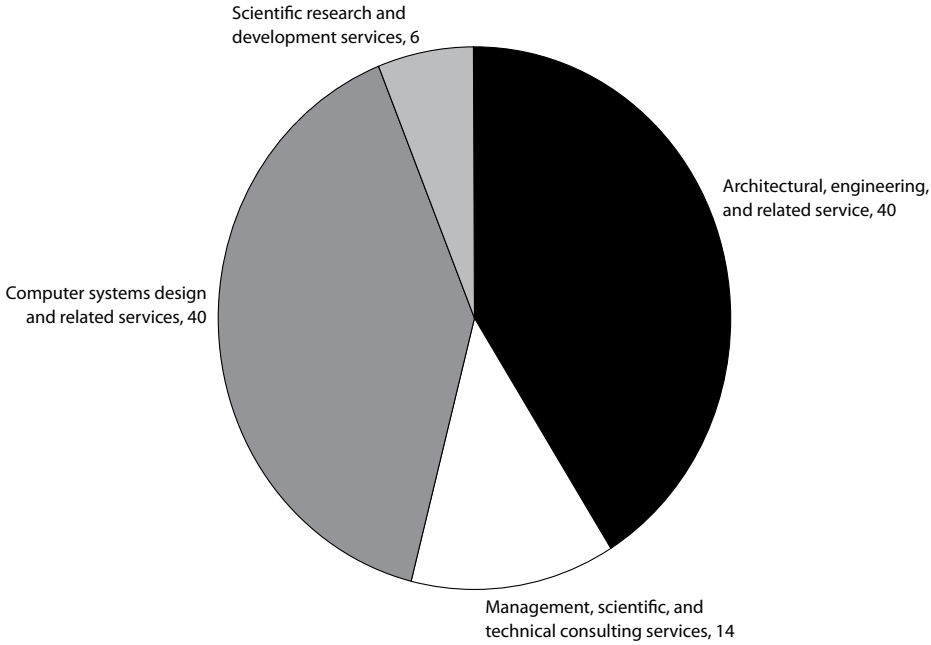


Table A.6 Covered transactions by country, 2005–07

Country	2005	2006	2007	Total, 2005–07
Australia	2	7	9	18
Austria	—	—	1	1
Bahrain	2	—	1	3
Belgium	—	2	1	3
Bermuda	2	1	—	3
Brazil	—	4	1	5
Canada	6	8	21	35
Cayman Islands	1	—	—	1
China	1	—	3	4
Denmark	1	—	—	1
Finland	—	3	1	4
France	9	9	7	25
Germany	2	4	6	12
Hong Kong	—	1	1	2
India	2	—	5	7
Ireland	—	1	1	2
Israel	1	9	6	16
Italy	1	3	3	7
Japan	3	6	1	10
Korea	—	1	—	1
Kuwait	1	2	2	5
Luxembourg	—	3	1	4
Malaysia	—	—	1	1
Mexico	—	2	—	2
Netherlands	—	4	7	11
Norway	1	1	1	3
Pakistan	—	2	—	2
Qatar	—	1	1	2
Russia	—	2	—	2
Saudi Arabia	—	1	1	2
Singapore	2	3	1	6
South Africa	—	—	1	1

(table contines next page)

Table A.6 Covered transactions by country, 2005–07 *(continued)*

Country	2005	2006	2007	Total, 2005–07
Spain	—	2	6	8
Sweden	1	1	—	2
Switzerland	1	1	6	8
Taiwan	—	—	3	3
United Arab Emirates	1	2	7	10
United Kingdom	24	23	32	79
Venezuela and Spain	—	2	—	2
Total	64	111	138	313

Table A.7 Covered transactions by country and sector, 2005–07

Country	Information	Manufacturing	Mining, utilities, and construction	Wholesale trade	Other	Total
Australia	6	3	5	4	—	18
Austria	—	1	—	—	—	1
Bahrain	2	1	—	—	—	3
Belgium	—	3	—	—	—	3
Bermuda	1	2	—	—	—	3
Brazil	—	4	1	—	—	5
Canada	21	7	5	2	—	35
Cayman Islands	—	1	—	—	—	1
China	1	3	—	—	—	4
Denmark	—	—	—	1	—	1
Finland	4	—	—	—	—	4
France	6	14	1	4	—	25
Germany	5	4	1	2	—	12
Hong Kong	—	2	—	—	—	2
India	7	—	—	—	—	7
Ireland	1	1	—	—	—	2
Israel	5	11	—	—	—	16
Italy	—	7	—	—	—	7
Japan	5	5	—	—	—	10
Korea	—	—	—	1	—	1
Kuwait	1	1	—	3	—	5
Luxembourg	3	—	—	1	—	4
Malaysia	—	1	—	—	—	1
Mexico	2	—	—	—	—	2
Netherlands	2	8	—	1	—	11
Norway	1	2	—	—	—	3
Pakistan	—	2	—	—	—	2
Qatar	—	—	2	—	—	2
Russia	—	2	—	—	—	2
Saudi Arabia	—	1	—	—	1	2
Singapore	3	3	—	—	—	6
South Africa	1	—	—	—	—	1
Spain	1	—	7	—	—	8

(table continues next page)

Table A.7 Covered transactions by country and sector, 2005–07
(continued)

Country	Information	Manufacturing	Mining, utilities, and construction	Wholesale trade	Other	Total
Sweden	2	—	—	—	—	2
Switzerland	2	6	—	—	—	8
Taiwan	—	3	—	—	—	3
United Arab Emirates	2	4	1	3	—	10
United Kingdom	28	44	4	3	—	79
Venezuela and Spain	—	2	—	—	—	2
Total	112	148	27	25	1	313

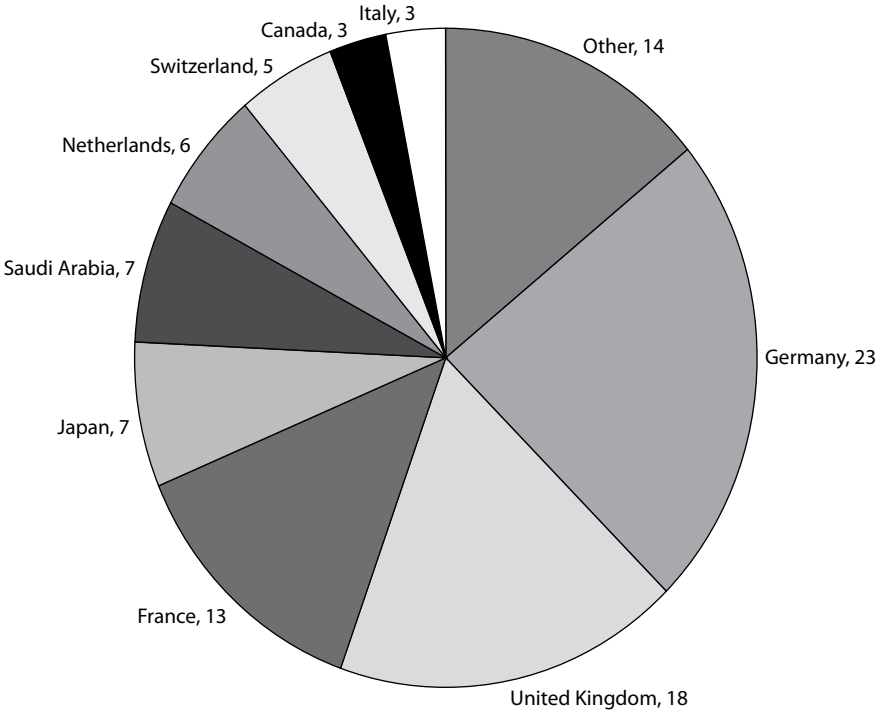
Table A.8 Foreign companies most active in acquiring US critical technology firms, 2006–07

Acquirer	Country	Number of acquisitions
Thomson Corporation	Canada	10
RAB Capital PLC	United Kingdom	10
Harris Computer Systems	Canada	8
SAP AG	Germany	8
Siemens AG	Germany	8
Reed Elsevier NV	United Kingdom	8
Nokia	Finland	7
Essilor International SA	France	7
Accenture Ltd.	Bermuda	6
Wolters Kluwer NV	Netherlands	6
Roche Holding AG	Switzerland	6
Laird Group PLC	United Kingdom	5
Stantec Inc.	Canada	4
Sonepar USA	France	4
Bayer AG	Germany	4
CDC Software	Hong Kong	4
Sony	Japan	4
Koninklijke Philips Electronic	Netherlands	4
Jobserve Ltd.	United Kingdom	4
Pearson PLC	United Kingdom	4
United Business Media PLC	United Kingdom	4
WPP Group PLC	United Kingdom	4

Table A.9 US critical technology transactions and deal value by country, 2006–07

Country	Number of deals	Deal value (billions of US dollars)
United Kingdom	203	28.4
Canada	170	5.6
Japan	58	11.8
Germany	55	36.1
France	49	20.1
India	34	1.4
Netherlands	34	9.7
Switzerland	31	8.6
Australia	28	3.3
Israel	22	1.1

Figure A.5 Total value of completed US critical technology transactions by country, 2006–07 (percent)



References

Bergsten, C. Fred, and Marcus Noland. 1993. *Reconcilable Differences? United States–Japan Economic Conflict*. Washington: Institute for International Economics.

Brander, James A., and Barbara J. Spencer. 1981. Tariffs and the Extraction of Foreign Monopoly Rents and Potential Entry. *Canadian Journal of Economics* 14, no. 3 (August): 371–89.

European Commission. 2008. Directorate-General for Competition (January). Brussels. Available at http://ec.europa.eu.

Gansler, Jacques. Forthcoming. *Democracy's Arsenal: Creating a 21st Century Defense Industry.* Cambridge, MA: MIT Press.

Graham, Edward M., and David M. Marchick. 2006. *US National Security and Foreign Direct Investment.* Washington: Institute for International Economics.

Graham, Edward M., and Paul R. Krugman. 1989 (2000 revised). *Foreign Direct Investment in the United States.* Washington: Institute for International Economics.

Hedrick, James B. 2003. Rare Earths. *US Geological Survey Minerals Yearbook*: 60.1–60.15. Washington: US Geological Survey. Available at http://minerals.usgs.gov.

Hufbauer, Gary Clyde, and Jeffrey J. Schott. 1985. The Soviet-European Gas Pipeline: A Case of Failed Sanctions. In *Multinational Corporations: The Political Economy of Foreign Direct Investment,* ed. Theodore H. Moran. Lexington, MA: D. C. Heath.

Hufbauer, Gary Clyde, Yee Wong, and Ketki Sheth. 2006. *US-China Trade Disputes: Rising Tide, Rising Stakes*. Policy Analyses in International Economics 78. Washington: Institute for International Economics.

Jackson, James K. 2007. *The Committee on Foreign Investment in the United States (CFIUS).* Washington: Congressional Research Service (July 23).

Krugman, Paul R., ed. 1986. *Strategic Trade Policy and the New International Economics.* Cambridge, MA: MIT Press.

Levenstein, Margaret C., and Valerie Y. Suslow. 2006. What Determines Cartel Success? *Journal of Economic Literature* XLIV (March): 43–95.

Marchick, David M., and Matthew Slaughter. 2008. *Global FDI Policy: Correcting a Protectionist Drift*. New York: Council on Foreign Relations (June).

Medeiros, Evan S., Roger Cliff, Keith Crane, James C. Mulvenon. 2005. *A New Direction for China's Defense Industry.* Santa Monica, CA: Rand Corporation.

Moran, Theodore H. 1990. The Globalization of America's Defense Industries: Managing the Threat of Foreign Dependence. *International Security* 15, no. 1 (Summer).

Moran, Theodore H. 2009 (forthcoming). *American Multinationals and American Economic Interests: New Dimensions to an Old Debate*. Working Paper. Washington: Peterson Institute for International Economics.

Tyson, Laura D'Andrea. 1992. *Who's Bashing Whom? Trade Conflict in High-Technology Industries.* Washington: Institute for International Economics.

US DOD (Department of Defense). 2005–07. *Annual Industrial Capabilities Reports to Congress*. Washington: Government Printing Office.

US DOD (Department of Defense). 2008. *Annual Report to Congress: Military Power of the People's Republic of China*. Washington: Government Printing Office.

US DOJ/FTC (Department of Justice/Federal Trade Commission). 2006. *Commentary on the Horizontal Merger Guidelines* (March). Washington. Available at www.usdoj.gov.

US Department of the Treasury. 2008a. Section 721 of the Defense Production Act of 1950. Committee on Foreign Investment in the United States Final Regulations, Issued November 14. Washington. Available at www.treas.gov (accessed on February 21, 2009).

US Department of the Treasury. 2008b. *Committee on Foreign Investment in the United States Annual Report to Congress.* Public Version (December). Washington. Available at www.treas.gov (accessed on June 18, 2009).

US GAO (General Accounting Office). 1991. *US Business Access to Certain Foreign State-of-the-Art Technology.* Washington.

US GAO (General Accounting Office). 1993. *Defense Industrial Base: An Overview of an Emerging Issue.* GAO/NSIAD-93-68. Washington.

US GAO (Government Accountability Office). 2005. *Industrial Security: DOD Cannot Ensure Its Oversight of Contractors under Foreign Influence Is Sufficient.* Report to the Committee on Armed Services, US Senate. GAO-05-681. Washington.

US GAO (Government Accountability Office). 2007. *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain*. Report to Congressional Requesters (September). GAO-07-1036. Washington.

US House of Representatives. 1991. *National Security Takeovers and Technology Preservation.* Hearings before the Subcommittee on Commerce, Consumer Protection, and Competitiveness of the Committee on Energy and Commerce, February 26 and June 12. Washington: Government Printing Office.

US Securities and Exchange Commission. 2008. 3Com Corporation, Proxy Statement Pursuant to Section 14(a) of the Securities Exchange Act of 1934 (January 24). Washington.

Index

Abramovich, Roman, 11
Accenture Ltd., 53*t*
access to supplies. *See* Threat I
acoustic signal processing system, 4, 30
acquisitions
  critical technology firms, 44
  DOJ/FTC guidelines for, 14, 33–34
advanced ceramic technology, withholding of, 10, 37
advanced manufacturing sector, 43
advanced material and processing sector, 43
aerospace and surface transportation sector, 44
Airbus, 35
Alcatel, 38
alternative sources
  availability of, 8, 11–13, 12*n,* 33
  legislative phrasing about, 4–5
  technology transfer and, 17
analytical tools, for evaluating three threats, 3–4
2008 Annual Report to Congress on the Military Power of the People's Republic of China (DOD), 26
antisubmarine warfare capabilities, 20–21
antitrust analysis, 3–4, 6
  concentration test in, 13–14, 34
  example of, 10
appliances sector, transactions in, 46*t*
application-specific integrated circuit (ASIC)-based engine, 27
architectural services sector, transactions in, 48*f,* 48*t*
ASML, 10*n,* 38
ATACM long-range missile, 16
Australia, transactions, 49*t,* 51*t,* 54*t*
Austria, transactions, 49*t,* 51*t*
autarchy, 7–8

Bahrain, transactions, 49*t,* 51*t*
Bain Capital, 6, 25–28
  Threat II and, 16–17
  Threat III and, 4–5
Baldrige, Malcolm, 9
Barrett, Craig, 10*n,* 38
Bayer AG, 53*t*
Belgium, transactions, 49*t,* 51*t*
Bell Labs, 38
Bentsen, Lloyd, 10
Bermuda
  critical technology firms, 44, 53*t*
  transactions, 49*t,* 51*t*
biotechnology sector, 43
blind trusts (special security agreements), 16, 30*n,* 30–31, 38
bloggers, on 3Com case, 27*n,* 28
Boeing, 35
Brazil, transactions, 49*t,* 51*t*
Bush administration, 25*b*

Canada
  critical industry mergers and acquisitions, 44

critical technology firms, 44, 53*t*
transactions, 42, 49*t*, 51*t*, 55*f*
deal value of, 54*t*
Canon, 9
case review process (CFIUS), 2*b*–3*b*
Caterpillar, 35
Cayman Islands, transactions, 49*t*, 51*t*
CDC Software, 53*t*
ceramic technology, withholding of, 10, 37
CFIUS. *See* Committee on Foreign Investment in the United States
chemicals sector, 43
transactions in, 46*t*
Chevron, 20
China
antisubmarine warfare capabilities, 20–21
Lenovo case, 5, 17–18
National Security Bureau, 28
People's Liberation Army, 19–20, 26, 28
Threat II and, 4
transactions, 49*t*, 51*t*
China National Offshore Oil Corporation (CNOOC), 6, 18–21
early cases previewing, 9, 12
Threat I and, 19
Threat II and, 20
Cisco Systems, 17, 27, 28, 37
Citgo, 25*b*
close substitutes
availability of, 8, 11–13, 12*n*, 33
legislative phrasing about, 4–5
technology transfer and, 17
CNOOC. *See* China National Offshore Oil Corporation
coal products sector, transactions in, 46*t*
collusion, 3, 13–14
commercial off-the-shelf (COTS) system, 30
Committee on Foreign Investment in the United States (CFIUS), 1, 2*b*–3*b*
case review process, 2*b*–3*b*
composition of, 2*b*
legislative coverage, 4–5, 36–37
strategic implications, 33–38
transactions (*See* transactions)
commoditization, 17
communications equipment manufacturing sector, transactions in, 47*f*, 47*t*
comparative advantage, 7–8
competitors, national security issues as advantage for, 9
compliance, monitoring of, 23, 38, 42–43
computer and electronic products sector, transactions in, 42, 46*f*, 46*t*, 47*f*, 47*t*
computer systems design sector, transactions in, 48*f*, 48*t*
concentration of suppliers, 8
energy supplies, 19
evaluation of, 10–14, 34
confidentiality violations, on CFIUS submissions, 27*n*
Congress, preference for national self-sufficiency, 7
construction sector, transactions in, 45*f*, 45*t*, 51*t*–52*t*
consulting services sector, transactions in, 48*f*, 48*t*
container terminals, 25*b*
"control," concept of, 4
control instruments sector, transactions in, 47*f*, 47*t*
Council of Economic Advisers, 2*b*
country. *See also specific country*
critical technology investment by, 44, 53*t*, 54*t*, 55*f*
transactions by, 42, 49*t*–52*t*
"critical," concept of, 5, 11, 13, 18
critical infrastructure
definition of, 4–5, 11, 33
foreign ownership of, 25*b*
responsibility for, 23, 38
critical technologies
classification of, 43–44
definition of, 5, 33, 43
employment share, 44
foreign direct investment in, 44, 53*t*, 54*t*, 55*f*
Crotale missile, 16
cyber warfare, 26

Datang, 26
deal value, critical technology transactions, 54*t*
DeepNines, 27
defense industries
foreign supplier base for, advantages of, 13
high-tech inputs, 9–10, 36–37
limitation of threats to, 6, 36–37
Threat I and, 13
Threat III and, 13*n*
Defense Production Act of 1950, Section 721, 2*b*, 4, 41
Defense Science Board, 7
Defense Security Service (DOD), 38
defensive mode, threat analysis in, 35
denial of access. *See* Threat I
Denmark, transactions, 49*t*, 51*t*
Department of Commerce, 2*b*, 11

Department of Defense (DOD), 2*b*, 12*n*
2008 Annual Report to Congress on the Military Power of the People's Republic of China, 26
Defense Security Service, 38
ITAR exemption, 17
proxy subsidiaries, 30*n*, 31
reverse engineering, 28
special security agreements, 16, 30*n*, 30–31, 38
Department of Energy, 2*b*
Department of Homeland Security (DHS), 2*b*, 24
Department of Justice, 2*b*, 10
mergers and acquisitions guidelines, 14, 33–34
Department of State, 2*b*
International Traffic in Arms Regulations (ITAR) categories, 17
Department of the Treasury, 44
Office of Investment Security, 2*b*
domestic ownership, maintenance of, 7–8
Dresser Industries, 8–9, 12, 13
Drexel, 37
DRS Technologies, 4, 6, 16, 28–31
Dubai Ports World controversy, 6, 24, 25*b*

economic externalities, 3–4, 35
economic rents, 3–4, 35
economies of scale, 7
electromedical instruments sector, transactions in, 47*f*, 47*t*
electronic products sector, transactions in, 42, 46*f*, 46*t*, 47*f*, 47*t*
Eller, 25*b*
employment, in critical technology industries, 44
"enemy" ("hostile"), 12
energy sector, 44
energy sources, new, development of, 20
energy supplies
European, 8–9, 12, 13, 37
US, 19–20
engineering services sector, transactions in, 48*f*, 48*t*
equivalence or nonequivalent treatment, 23–24
espionage. *See* Threat III
"essential," concept of, 5
Ethernet routers and switches, 28
Europe. *See also specific country*
Threat I case in, 8–9, 12, 13
European Commission Directorate-General for Competition, 14, 34
europium, 21
"evergreen" reservations, 38
Evraz, 11
Executive Order 11858, 2*b*
Exon-Florio provision, 7, 9
expertise, leakage of. *See* Threat II
export control regime, 17, 30
extended range missile interceptor (ERINT), 16
externalities, 3–4, 35
Exxon-Mobil, 37

fabricated metal products sector, transactions in, 46*t*
Fairchild Semiconductor, 9
Federal Trade Commission, mergers and acquisitions guidelines, 14, 33–34
"fifth column," 23
financial derivatives, foreign ownership of, 24
Finland
critical technology firms, 44, 53*t*
Nokia, 44
transactions, 49*t*, 51*t*
Finmeccanica, 4, 6, 16, 28–31
foreign direct investment, in critical technology industries, 43–44
Foreign Investment and National Security Act of 2007 (FINSA), 2*b*, 4, 5, 41, 43
foreign-owned facilities, monitoring of, 23, 38, 42–43
foreign ownership, of financial derivatives, 24
foreign suppliers
dependence on, 11
diversified base of, advantages of, 13
France
critical industry mergers and acquisitions, 44
critical technology firms, 44, 53*t*
Dresser case, 8–9, 12, 13, 37
Thomson-CSF case, 5, 12*n*, 15–17, 30
transactions, 42, 49*t*, 51*t*, 55*f*
deal value of, 54*t*
free trade, benefits of, 8
Fujitsu, 9

gas pipelines
Soviet, 8–9, 12, 13, 37
US, 19–20
Gazprom, 37
General Accounting Office (GAO), 10, 10*n*, 11
General Electric (GE), 8–9, 12

Germany
critical industry mergers and acquisitions, 44
critical technology firms, 44, 53*t*
transactions, 49*t*, 51*t*, 55*f*
deal value of, 54*t*
global market, concentration test in, 13
global ownership, versus domestic ownership, 7
guidelines, for CFIUS decision making, 14, 33–34
Gulf War, 11, 16

hardware network, 25–28
Harris Computer Systems, 53*t*
H3C, 26
headquarters effect, 18
Hercules, 10
Herfindahl-Hirschman Index (HHI), 6, 34
high-tech industries, Japanese competition for, 9
high-tech inputs, for defense industries, 9–10, 36–37
home country, transfer of activities to, 18
home-country directives, 13, 37
homeland security, definition of, 4–5
Homeland Security Council, 2*b*
Hong Kong
critical technology firms, 44, 53*t*
transactions, 49*t*, 51*t*
"hostile" ("enemy"), 12
House Appropriations Committee, 25*b*
Huawei Technologies, 6, 25–28
Threat II and, 16–17
Threat III and, 5
Hunter, Duncan, 18*n*
Hussein, Saddam, 11

IBM, 5, 17–18, 27
India
critical industry mergers and acquisitions, 44
transactions, 49*t*, 51*t*, 54*t*
industry sector. *See also specific sector*
transactions by, 42, 45*f*, 45*t*, 51*t*–52*t*
infiltration. *See* Threat III
information sector, 43
mitigation measures in, 43
transactions in, 42, 45*f*, 45*t*, 51*t*–52*t*
Intel, 17, 37, 38
International Energy Agency (IEA), 20
International Traffic in Arms Regulations (ITAR) categories, 17
investigations (CFIUS), 41, 45*t*
investment
in critical technology industries, 43–44, 53*t*, 54*t*, 55*f*
free flows of, benefits of, 8
Iraq, 11, 16
Ireland, transactions, 49*t*, 51*t*
Israel, transactions, 49*t*, 51*t*, 54*t*
Italy
Finmeccanica case, 4, 6, 16, 28–31
transactions, 49*t*, 51*t*, 55*f*

Japan
critical industry mergers and acquisitions, 44
critical technology firms, 44, 53*t*
Ministry of International Trade and Industry, 10
transactions, 49*t*, 51*t*, 55*f*
deal value of, 54*t*
US concerns about, 9, 13
Jobserve Ltd., 53*t*
Juniper Networks, 27

Koninklijke Philips, 44, 53*t*
Korea, transactions, 49*t*, 51*t*
Kuwait, transactions, 49*t*, 51*t*
Kyocera, 10, 37

Laird Group PLC, 53*t*
lanthanides, 21
Lautenberg, Frank, 24
leading edge capabilities, 17
leakage. *See* Threat II
legislative language, 4–5, 36–37
Lenovo, 5, 17–18
letters of assurance, 24, 42–43
Libya, 16
line-of-sight antitank (LOSAT) missile, 16
lithography equipment, 9–10, 10*n*, 36
Lockheed, 16
LTV Corporation, 5, 12*n*, 15–17, 30
Lucent, 38
Luxembourg, transactions, 49*t*, 51*t*

machinery sector, transactions in, 46*f*, 46*t*
Malaysia, transactions, 49*t*, 51*t*
management services sector, transactions in, 48*f*, 48*t*
manipulation of access. *See* Threat I
manufacturing sector
mitigation measures in, 43
transactions in, 42, 45*f*, 45*t*, 46*f*, 46*t*, 51*t*–52*t*
marine systems sector, 44

market concentration, 8
  energy supplies, 19
  evaluation of, 10–14, 34
market function, analysis of, 8
McAfee, 27
measuring instruments sector, transactions in, 47*f*, 47*t*
meltdown mechanism, 24
mergers and acquisitions
  critical technology firms, 44
  DOJ/FTC guidelines for, 14, 33–34
metals sector, transactions in, 46*t*
Mexico, transactions, 49*t*, 51*t*
microelectronics sector, 43
military advantage, 3–4
Military Critical Technologies List, 43
military industry. *See* defense industries
military-related electronics sector, 43
mining sector, transactions in, 45*f*, 45*t*, 51*t*–52*t*
missile programs, 10, 16, 37
mitigation process, 29–30, 31
  measures taken, 42–43
Molycorp, 20–21
monopolistic pricing, 10
Mountain Pass (California), 20–21
multiple launch rocket system (MLRS), 16

National Economic Council, 2*b*
national security
  definition of, 4–5, 36
  evaluation of, 11–12, 26
National Security agency, 28
national security agreements (NSAs), 42–43
National Security Council, 2*b*
national self-sufficiency, 7–8
National Semiconductor, 9
navigational instruments sector, transactions in, 47*f*, 47*t*
Netherlands
  ASML case, 10*n*, 38
  critical technology firms, 44, 53*t*
  Koninklijke Philips, 44
  transactions, 49*t*, 51*t*, 55*f*
    deal value of, 54*t*
NFR Security, 27
Nikon, 9–10, 12, 13
Nippon Sanso, 10, 12
NitroSecurity, 27
Nokia, 44
nonmetallic mineral products sector, transactions in, 46*t*
North American Industry Classification System (NAICS), 43
Norway, transactions, 49*t*, 51*t*
notices, 3*b*, 41, 45*t*. *See also* transactions

Office of Investment Security (Department of Treasury), 2*b*
Office of Management and Budget, 2*b*
Office of Science and Technology Policy, 2*b*
Office of the US Trade Representative, 2*b*
oil industry, 6, 18–21
oligopoly theory, 34
Omnibus Trade Act of 1988, 7
Operations Desert Shield/Desert Storm, 11, 16
optical lithography equipment, 9–10, 10*n*, 36
Oregon Steel, 5, 11–12

Pakistan, transactions, 49*t*, 51*t*
Pearson PLC, 53*t*
Peninsular and Oriental Steam Navigation Company (P&O), 25*b*
People's Liberation Army (PLA), 19–20, 26, 28
Perkin Elmer, 9–10, 12
personal computer (PC) industry, 5, 17–18
petroleum products sector, transactions in, 46*t*
Pfizer, 35
plastic sector, transactions in, 46*t*
Poland, 8
political advantage, 3–4
political protectionism, safeguards against, 36
port-related operations, 25*b*
presidential decisions, 41, 45*t*
private companies, as pawns in policy struggles, 13
professional, scientific, and technical services sector, 43–44
  transactions in, 48*f*, 48*t*
protectionism, safeguards against, 36
proxy subsidiaries, 30*n*, 31
public authorities, monitoring of foreign-owned facilities by, 23, 38, 42–43
publishing industry, transactions in, 42

Qatar, transactions, 49*t*, 51*t*
quasi-monopolistic supplier, 3, 35
  example of, 10
  versus less capable national producer, 10*n*

RAB Capital PLC, 53*t*
radio search and rescue signal equipment, 11

Radware, 27
Rand Corporation, 26
rare earths, 20–21, 21*n*
Reagan administration, 8, 13
receiver control software (RCS), 30
Reed Elsevier NV, 53*t*
Reflex Security, 27
remediation, 37–38
  ASML-Silicon Valley Group case, 10*n*
  in European gas pipeline case, 9, 37
  Threat III and, 24
rents, 3–4, 35
Ren Zhengfei, 26
research and development services sector, transactions in, 48*f*, 48*t*
reverse engineering, 28
Roche Holding AG, 53*t*
rubber products sector, transactions in, 46*t*
Russia, transactions, 49*t*, 51*t*
Russian oligarchy, 11–12

sabotage. *See* Threat III
sales discrimination, 10
SAP AG, 53*t*
Saudi Arabia, transactions, 49*t*, 51*t*, 55*f*
scandium, 21
Schlumberger, 9
scientific services sector, 43–44
  transactions in, 48*f*, 48*t*
Section 721 (Defense Production Act of 1950), 2*b*, 4, 41
security clearances, 30*n*
security compartmentalization, 38
seismic technology, 21
Sematech, 10
semiconductor industry sector, 9–10, 10*n*, 13, 36–37, 43
  transactions in, 42, 47*f*, 47*t*
Semi-Gas Systems, 10, 12
Senate Armed Services Committee, Subcommittee on Defense Industry and Technology, 15*n*
separate-and-different treatment, 23–24
September 11, 2001 attacks, 25*b*
Siemens AG, 44, 53*t*
Silicon Valley Group, 10*n*, 38
silicon wafers, 9–10
Singapore, transactions, 49*t*, 51*t*
software network, 25–28
Sonepar USA, 53*t*
Sony, 53*t*
Sourcefire, 27
South Africa, transactions, 49*t*, 51*t*
Soviet gas pipeline, 8–9, 12, 13, 37
space systems sector, 44
Spain, transactions, 50*t*, 51*t*
special access programs (SAPs), 29
specialization, 7
special security agreement (SSA), 16, 30*n*, 30–31, 38
Standard Industrial Classification (SIC), 43
standards, for CFIUS decision making, 14, 33–34
Stantec Inc., 53*t*
steel industry, 5, 11–12, 12*n*
"stepper" industry, 9–10
StillSecure, 27
strategic trade theory, 3–4, 6, 35–36
Subcommittee on Defense Industry and Technology (Senate Armed Services Committee), 15*n*
subsidiaries (US), establishment of, 30–31, 38
supplies, denial or manipulation of access to. *See* Threat I
Sweden, transactions, 50*t*, 52*t*
switching costs, 8, 12*n*, 13, 33
  energy supplies, 19
Switzerland
  critical technology firms, 44, 53*t*
  transactions, 50*t*, 52*t*, 55*f*
    deal value of, 54*t*

Taiwan, transactions, 50*t*, 52*t*
takeover plans, national security issues as advantage for, 9
target acquisition/designation, 30
technical services sector, 43–44
  transactions in, 48*f*, 48*t*
technology
  free flows of, benefits of, 8
  leakage of (*See* Threat II)
telecommunications sector, 43
  transactions in, 42
terminology (CFIUS), 4–5, 36–37. *See also specific term*
textile product mills sector, transactions in, 46*t*
Thomson Corporation, 44, 53*t*
Thomson-CSF, 5, 12*n*, 15–17, 30
threat(s)
  CFIUS legislation coverage, 4–5, 36–37
  evaluation tools, 3–4, 33–38
  interrelationships between, 6, 18–21, 25–41
  overview of, 1, 5–6
Threat I (denial or manipulation of access to supplies), 1, 5, 7–14

case analysis, 8–11
defense industries and, 13
evaluation tools, 3–4, 33, 35
interrelationship with other threats, 18–21, 26, 29
legislative phrasing about, 4, 36–37
lessons learned, 12–14
limitation to defense industries, 6, 36–37
Threat II ("leakage"), 1, 5, 15–21
case analysis, 5–6, 15–18
evaluation tools, 3–4, 16–17, 33, 35
interrelationship with other threats, 18–21, 26–27, 29–30
legislative phrasing about, 4, 36–37
Threat III (sabotage and espionage), 1, 6, 23–31
defense industries and, 13*n*
evaluation tools, 3–4, 33
interrelationship with other threats, 27–28, 29–30
legislative phrasing about, 4–5, 36–37
limitation to defense industries, 6, 36–37
threat suppression engine, 27
3Com, 25–28
Threat I and, 26
Threat II and, 16–17, 26–27
Threat III and, 5, 27–28, 36–37
TippingPoint, 27
Tomahawk cruise missile program, 10, 37
Top Layer Networks, 27
transactions (2005-07), 41–55
by country, 42, 49*t*–52*t* (*See also specific country*)
deal value of, 54*t*
by industry sector, 42, 45*f*, 45*t*, 51*t*–52*t* (*See also specific sector*)
notices submitted, 45*t*
transportation equipment sector, transactions in, 46*f*, 46*t*
United Arab Emirates, transactions, 50*t*, 52*t*
United Business Media PLC, 53*t*
United Kingdom
critical industry mergers and acquisitions, 44
critical technology firms, 53*t*
transactions, 42, 50*t*, 52*t*, 55*f*
deal value of, 54*t*
Unocal, 6, 18–21
early cases previewing, 9, 12
seismic technology, 21
US Congress, preference for national self-sufficiency, 7
US Geological Survey, 21
US government departments. *See specific department*
US Steel, 35
US subsidiaries, establishment of, 30–31, 38
utilities sector, transactions in, 45*f*, 45*t*, 51*t*–52*t*

Venezuela, transactions, 50*t*, 52*t*
voluntary notices, 3*b*, 41. *See also* transactions

Weinberger, Casper, 9
White House Office of Science and Technology Policy, 43
wholesale trade sector, transactions in, 45*f*, 45*t*, 51*t*–52*t*
withdrawn notices, 41, 45*t*
Wolter Kluwer NV, 53*t*
World Bank, 20
WPP Group PLC, 53*t*

yttrium, 21

Zhongxing, 26