Peterson Institute for International Economics

In Brief

Three Threats: An Analytical Framework for the CFIUS Process

Theodore H. Moran • August 2009 • 66 pp. ISBN Paper 978-0-88132-429-7 • $17.95

Under what conditions might foreign acquisition of a US company constitute a genuine national security threat to the United States? How should analysts and strategists at the Committee on Foreign Investment in the United States (CFIUS), together with congressional overseers, assess risks and threats to distinguish between the serious and the inconsequential?

Theodore Moran distinguishes between three categories of potential threats that foreign acquisition of a US company might pose. 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 the 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 the 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.

THREAT I: DENIAL OF GOODS OR SERVICES BY A FOREIGN-CONTROLLED SUPPLIER

Three criteria are necessary for there to be a credible likelihood that a foreign-controlled supplier could either withhold a good or service at great cost to the economy or provide it 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 there are many suppliers, and they 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.

Moran draws on historical and contemporary cases, using foreign acquisitions in the semiconductor, steel, and oil industries, to clarify what is "critical" to the United States. Whether for semiconductor equipment or other crucial inputs, such as steel, to the 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, blackmail, or the placement of limitations on access or use to be credible, the necessary condition is the unavailability of substitutes.

THREAT II: LEAKAGE OF TECHNOLOGY OR EXPERTISE TO A FOREIGN-CONTROLLED ENTITY

The question when assessing whether a transaction poses Threat II 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? As in the case of Threat I, a concentration test can also be used to assess Threat II, because it could 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. Moran uses two classic cases—the proposed acquisition of the 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.

He then applies Threat I and Threat II tests to analyze the **Chinese oil company CNOOC's proposed acquisition of**

Unocal, which raised concern that CNOOC might divert some or even all of Unocal's energy supplies exclusively to meet Chinese needs and might obtain sensitive technology, particularly to enhance its antisubmarine capabilities. Based on Threat I criteria, a diversion of oil supplies by China 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. 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.

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, 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. 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.

THREAT III: FOREIGN ACQUISITIONS AS A CHANNEL FOR INFILTRATION, SURVEILLANCE, AND SABOTAGE

Threat III is a separate category 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 a "fifth column" might be able to penetrate the newly foreign-owned enterprise.

The Dubai Ports World (DPW) case raised this third concern. DPW manages container terminals and other port-related operations in 14 countries and is based in the United Arab Emirates. In 2005 it 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 George W. Bush and his cabinet members tried to quell the protest without success.

Three charges were leveled against the DPW 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 DPW 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. Faced with overwhelming opposition in Congress, DPW conceded on March 9, 2006, stating that it would sell the US port facilities acquired from P&O to a US-controlled firm.

Prior to initial CFIUS approval, the Department of Homeland Security (DHS) negotiated a "letter of assurances" with DPW, stipulating that the company would operate all US facilities with US management, designate a DPW 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. 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.

Moran also explores the interrelationships between the three threats: Bain Capital's failed attempt to acquire 3Com, with a minority interest for Huawei Technologies of China, provides the opportunity to investigate the interaction between Threats I, II, and III, as does Finmeccanica's successful takeover of DRS Technologies.

FOREIGN INVESTMENT IN US CRITICAL TECHNOLOGY SECTORS

The US Treasury Department reported that as of the end of 2006, 23 percent of the stock of total foreign direct investment was in sectors that include critical technologies (e.g., microelectronics, biotechnology, semiconductor fabrication equipment, information and communications, space and marine systems, and aerospace and surface transportation)—up from 19 percent in 1997. Twenty-two foreign companies completed four or more acquisitions involving US critical technology firms in 2006–07 (table 1 shows the top 10 companies). Investors from the United Kingdom, Canada, Germany, France, and Japan dominated mergers and acquisitions activity in US critical technology sectors.

Table 1 Top ten foreign companies most active in acquiring US critical technology firms, 2006–07

Acquiror	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

SUMMING UP

To find out if a foreign transaction poses any or all of the three threats, CFIUS strategists and congressional watchdogs should first determine 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.

How accurately can CFIUS estimate whether a credible threat exists? Are there standards to guide CFIUS decision making? Moran takes a critical look at analytical tools that might aid CFIUS deliberations, namely, the Herfindahl-Hirschman concentration index (which is the sum of the squares of the market shares of all market participants) as used in antitrust cases and strategic trade theory. This index may be used 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. Moran concludes that ultimately, a vast majority of foreign acquisitions pose no credible threat to US national security.

To learn more about this book, visit http://bookstore.piie.com/book-store/4297.html
To learn more about Theodore H. Moran, visit http://www.piie.com/staff/author_bio.cfm?author_id=56