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.