4

FDI and National Security: Separating Legitimate Threats from Implausible Apprehensions

Foreign direct investment (FDI) that takes place through acquisition of an existing company in the home economy has long been a subject of particular sensitivity around the world, with frequent allegations that the outcome might negatively affect the national security of the home country. But what kind of acquisition would constitute a credible threat to national security? When would adverse national security consequences be implausible?

The US experience since the initial attachment of the Exon-Florio provision to the Omnibus Trade Act of 1988 shows that perceived threats to national security from foreign acquisition of a US company fall into three distinct categories.[1] The first category of threat (Threat I) is that the proposed acquisition would make the United States dependent on a foreign-controlled supplier for goods or services crucial to the functioning of the US economy—including, but not exclusively, the functioning of the defense industrial base—who could delay, deny, or place conditions on providing those goods or services. The second category of threat (Threat II) is that the proposed acquisition would allow transfer of technology or other expertise to a foreign-controlled entity that the entity or its government could deploy in a manner harmful to US national interests. The third category of threat (Threat III) is that the proposed acquisition would allow insertion of some capability for infiltration, surveillance, or sabotage—through a human or nonhuman agent—into the provision of goods or services crucial to the functioning of the US economy, including, but not exclusively, the functioning of the defense industrial base. The evolution of directives given to the Committee on Foreign Investment in the United States (CFIUS) from the Exon-Florio period through the latest Foreign Investment and National Security

1. This chapter draws on Moran (2009).

© Peterson Institute for International Economics | www.piie.com

Act (FINSA) regulations has not, however, kept up with the understanding of what constitutes a potential threat to national security or appreciated the relatively rare circumstances in which such a threat might be credible.

Threat I: Denial or Manipulation of Access

The pressures that led to the original Exon-Florio provision in 1988 arose from a broad concern about the possible decline of US high-technology industries, aggravated by aggressive competition from Japan. From the 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.

Fairchild Semiconductor

The immediate impetus for the passage of the Exon-Florio provision was the proposed sale of US company Fairchild Semiconductor by Schlumberger of France to Fujitsu in 1987. Commerce Secretary Malcolm Baldrige joined Defense Secretary Caspar Weinberger in arguing that the sale would give Japan control over a company that was 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-technology inputs, and Fujitsu withdrew its bid for Fairchild. Shortly thereafter National Semiconductor acquired Fairchild at a substantial discount from the Japanese acquisition price, setting a precedent for the China National Offshore Oil Corporation (CNOOC)–Unocal case in 2005. 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 criticism of the proposed acquisition rested on the premise that the target firm was in an industry crucial to the US economy and to US defense, with "crucial" defined in a commonsense manner that there would be a large negative effect if the economy had to do without the goods and services in question. There was no careful analysis of the conditions under which supply could be manipulated or withheld, or whether foreign corporate or government efforts to manipulate or withhold supply would have any practical effect. This changed in 1989 with the battle over a proposal by Nikon, a Japanese company, to acquire US company Perkin-Elmer's stepper division.

Perkin-Elmer

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 the global market for optical lithography and Canon, also a Japanese company, controlled another fifth (Bergsten and Noland 1993). If the acquisition were allowed, US producers would be highly constrained in where they could purchase machinery to

© Peterson Institute for International Economics | www.piie.com

etch microcircuits on semiconductors. The sale would effectively place quasi-monopoly power in the hands of the new owner, and by extension, the new owner's home government. Under the glare of scrutiny and political concerns, the acquisition did not proceed. The novel insight from the Perkin-Elmer case was that the term "crucial"—namely, the cost of doing without—had to be joined with parallel considerations: that there be a credible likelihood that a good or service could be withheld at great cost to the economy, or that the suppliers or their home governments could place conditions upon the provision of the good or service, which meant that the industry had to be tightly concentrated, the number of close substitutes limited, and the switching costs high.

The debate about Japanese company Nippon Sanso's proposal to acquire US firm Semi-Gas Systems in 1990 incorporated even more formally a methodology based on concentration of suppliers. The CFIUS process originally approved the sale of Semi-Gas by Hercules, its US parent company. 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 therefore the Department of Justice would lodge an antitrust challenge to the proposed sale. The degree of market concentration raised not just the possibility of monopolistic pricing but the specter of other forms of discrimination in sales behavior. Once again US semiconductor firms, as well as Sematech, the Pentagon-supported industry consortium with the objective of boosting the competitiveness of the US computer chip manufacturing industry, were justifiably wary of finding themselves at the mercy of a foreign supplier of the specialized cabinets that store and distribute toxic gases used to make chips.[2]

Senator Lloyd Bentsen 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 1991 US General Accounting Office (GAO 1991) report did not uncover convincing support for these assertions or for other illegal or predatory behavior on the part of Japanese suppliers. But concerns 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 (MITI), under pressure from Socialist members of the Diet, did force Dexel, the American subsidiary of Japanese firm Kyocera, to withhold advanced ceramic technology from the US Tomahawk cruise missile program.[3]

---

2. 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 analytic problem. In this case, however, prominent US industry figures including Craig Barrett, CEO of Intel, lobbied in favor of the acquisition. The dilemma lay between becoming dependent on a quasi-monopolistic foreign supplier and relying on a less capable (and perhaps failing) national producer.

3. National Security Takeovers and Technology Preservation, Hearings before the Subcommittee on Commerce, Consumer Protection, and Competitiveness of the Committee on Energy and Commerce, House of Representatives, February 26 and June 12, 1991, 179.

© Peterson Institute for International Economics | www.piie.com

Oregon Steel

The recognition that a proposed acquisition taking place in an industry identified as crucial was insufficient justification to block the acquisition emerged even more clearly in the case of a Russian oligarch's proposal to acquire Oregon Steel. In this case "crucial" was sometimes replaced with "critical," with the same implication of a high cost to the national economy if supply were manipulated or withheld. Would the acquisition of Oregon Steel in 2006 by the Russian company Evraz, which had close ties to Roman Abramovich, a Russian billionaire who enjoyed intimate relations with the Kremlin, pose a national security threat to the United States?

Following the methodology outlined above, for a foreign acquisition to pose a threat of the United States becoming dangerously dependent on a foreign supplier, CFIUS strategists have to evaluate both whether the good or service foreigners provide is crucial to the functioning of the US 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 providing 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 likewise 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 the global steel trade. Alternative sources of supply are widely dispersed, with 10 countries exporting more than 10 million metric tons[4] and 20 additional suppliers exporting more than 5 million metric tons.

The steel industry is vital to US national economic and security interests. But the multiplication of sources of supply around the world means that there is no realistic likelihood that an external supplier, or group of suppliers, could withhold steel from US purchasers or place conditions on US purchasers or the US government before delivery. The globalization of steel production allows US users to take advantage of the most efficient and lowest-cost sources of supply without a nagging worry that somehow the United States is becoming too dependent on foreigners. Evraz acquired Oregon Steel in 2006. The analytics applied in the Oregon Steel case could just as easily apply in assessing China's Angang Steel Company's proposed $175 million investment in 2010 to acquire a 20 percent stake in a rebar plant being built by a US company, Steel Development Company, in Amory, Mississippi—from which Angang backed away in the face of pressure from US lawmakers.

4. The 10 countries are Japan, Russia, Ukraine, Germany, Belgium-Luxembourg, France, South Korea, Brazil, Italy, and Turkey.

© Peterson Institute for International Economics | www.piie.com

Threat II: Leakage of Sensitive Technology or Know-How

In almost all proposed acquisitions, it would be odd if the takeover did not offer the foreign parent corporation some new production or managerial expertise, giving the home government of the foreign parent an opportunity to command that the expertise be deployed in ways the home government desired. It would be equally odd if the additional production or managerial expertise did not, in some marginal way, strengthen the home government's national defense capabilities, including its military. Thus the second test interacts with the first. How broadly available is the additional production or managerial expertise involved? How big a difference would the acquisition make for the new home government?

LTV Missile Business

The prototypical illustration of potentially worrisome technology transfer can be found in the landmark case of the proposed 1992 acquisition of US company Ling-Temco-Vought's (LTV) missile business by Thomson-CSF of France.[5] The LTV Corporation found itself in bankruptcy due to underfunded pension obligations associated with the parent company's steelmaking operations. To raise cash, a federal bankruptcy court in New York considered proposals from Martin Marietta, Lockheed, and Thomson-CSF to purchase LTV's missile division and approved sale to Thomson. 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. However, three product lines—the Multiple Launch Rocket System (MLRS) launcher, the Army Tactical Missile System (ATACM) longer-range rocket launcher, and the Line-of-Sight Anti-Tank (LOSAT) missile—had few or no comparable substitutes, and one—the Extended Range Interceptor (ERINT) antitactical missile—included highly classified technology that was at least a generation ahead of rival systems and virtually unique at the time. It is unclear 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 in any case had a long history of closely following French government directives. The potential for sovereign conflict over the disposition and timing of Thomson-CSF sales, should the LTV missile division become part of the group, was substantial. Prior 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 offered Iraq advance warning in the first Gulf War.

5. Materials prepared by Theodore H. Moran for the Subcommittee on Defense Industry and Technology, Senate Armed Services Committee, April 30, 1992.

© Peterson Institute for International Economics | www.piie.com

The Department of Defense (DOD) initially informed Congress that the Pentagon would insist upon a special security agreement (SSA), or blind trust, to perform the security work on LTV programs, an arrangement Thomson-CSF at first opposed but ultimately accepted. CFIUS rejected the proposed acquisition when Thomson and the Pentagon failed to reach agreement on how to ensure that sensitive US technology did not seep through in any way to the new French parent. Thus the methodology for determining whether a foreign acquisition might threaten to provide a channel for some unacceptable leakage of technology or other know-how follows the same path as already outlined. The key lies in calculating the concentration or dispersion of the particular capabilities that the acquired entity possesses. When the entity presides over some unique or very tightly held capabilities that could damage US national interests if deployed, the threat is genuine.

The above analytics are helpful in understanding Lenovo's proposal to acquire IBM's PC business and Huawei's proposal to take a stake in 3Com. They also play a subtle role in the evaluation of CNOOC's proposal to acquire Unocal.

Threat III: Infiltration, Espionage, and Disruption

The 2005 Dubai Ports World (DP World) case brought to the fore an additional concern, namely, that a foreign acquisition might provide a setting in which the new owner was less than vigilant in preventing hostile forces from infiltrating the operations of the acquired company, or might even be complicit in facilitating surveillance or sabotage. In 2005 DP World sought to acquire the Peninsular and Oriental Steam Navigation Company (P&O), a British firm. 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. CFIUS initially approved the acquisition, but the deal later fell through after considerable public political pressure from US lawmakers.

The issue was not whether foreign ownership of a given service provider (e.g., ports administration), infrastructure network (e.g., telecommunications), or facility (e.g., a petrochemical plant) might lead to the new owner or the owner's home government denying services, or whether sensitive technology or other management capabilities might be transferred to the new owner or the owner's home government. Instead, concerns focused on whether foreign ownership offered an increased likelihood that what Edward Graham and David Marchick (2006) have called a "fifth column" might be able to penetrate the newly foreign-owned structure. Foreign acquisition might afford the new owner's government a platform for clandestine observation or disruption.

In addition to rejecting a proposed acquisition, CFIUS may deal with Threat III–type cases through remediation utilized for foreign takeovers when classified technologies and materials are involved, such as a requirement to set separate compartmentalized divisions within the company where US

© Peterson Institute for International Economics | www.piie.com

citizenship and special security vetting are required. As part of the process that led to the first CFIUS approval, the Department of Homeland Security negotiated a letter of assurances with DP World, stipulating that Dubai Ports would operate all US facilities with US management, designate a corporate officer with DP World 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 as US agencies requested (Graham and Marchick 2006). But public outcry against DP World ownership was sufficiently great that this mitigation agreement was dismissed out of hand, and the parent company withdrew its offer. Concerns about infiltration, espionage, and possible disruption reemerge in Huawei's proposal to take an ownership stake in 3Com.

Applying the Three-Threat Prism to Proposed Chinese Acquisitions

Lenovo's Acquisition of IBM's PC Business

Did Lenovo's acquisition of IBM's PC business in 2005 pose a credible national security threat to the United States? Regarding Threat I (denial) and Threat II (leakage of sensitive technology), competition among personal computer producers is sufficiently intense that basic production technology is considered commoditized. More than a dozen producers compete for 50 percent of the PC market, with none showing a predominant edge for long. It is far-fetched to think that Lenovo's acquisition of IBM's PC business represented a leakage of sensitive technology or provided China with military-application or dual-use capabilities that were not readily available elsewhere. Nor could Lenovo manipulate access to PC supplies in any way that would matter, as purchasers could simply shift to Dell, Hewlett-Packard, or any one of a number of other sellers. As for Threat III (infiltration, espionage, and disruption), any purchasers who feared bugs or surveillance devices within Lenovo PCs could purchase computers from other suppliers in whom they had more confidence.

Angang Steel Proposed Acquisition of a Stake in Steel Development Company

As suggested earlier, the analytics of Angang Steel Company's proposed $175 million investment to acquire 20 percent ownership of Steel Development Company in Amory, Mississippi, is even more straightforward, even though the acquisition did not occur. As the Angang investment would create a new company, not acquire a share in an established one, CFIUS would not have jurisdiction. But the threat framework is nonetheless useful. Steel is most certainly critical to the US economy and the US defense industrial base. But sources of supply are highly competitive and switching costs are low, so Threat

© Peterson Institute for International Economics | www.piie.com

I is not worrisome. Rebar steel technology is commercially widespread, so Threat II does not apply. And a 20 percent ownership stake provides a poor platform for Threat III's preoccupation with sabotage. In the end, it was not careful threat assessment that led investors to abandon the project, but public uproar, including from established US steel companies for which the project would constitute a modern low-cost competitor.[6]

CNOOC's Proposed Acquisition of Unocal

The three threat assessment tools provide for a rigorous analysis of CNOOC's proposed acquisition of US oil company Unocal in 2005, which the Chinese company withdrew after substantial US political pressure. Looking solely at the question of whether oil is crucial for the functioning of the US economy and military, the answer is clearly yes. For many, this meant the case was closed.[7] From an analytical perspective, however, much was left to be considered, such as the concentration of alternative suppliers and potential switching costs, as well as potential leakage of sensitive technologies and managerial expertise.

In 2004 Unocal produced 159,000 barrels of oil per day (70,000 barrels per day in the United States) and 1.51 billion cubic feet of gas per day (577 million cubic feet per day in the United States); 33 percent of its oil and natural gas production was within the United States and 67 percent outside. Unocal had proven reserves of 659 million barrels of oil and 6.658 trillion cubic feet of natural gas. Of these reserves, 26 percent were within the United States and 74 percent outside. Concern was expressed that CNOOC might divert Unocal's energy supplies exclusively to meet Chinese needs. In the extreme, critics feared that CNOOC might reroute Unocal's US production back to China. This would be a highly complicated and expensive undertaking, as US pipelines across western states flow west to east; oil from the Gulf of Mexico would have to be shipped by tanker through the Panama Canal. But if it were accomplished, would this outcome harm the United States?

The diversion would constitute a threat to US interests only if sources of supply were tightly concentrated and switching costs high. But 21 countries—15 of them not members of the Organization of Petroleum Exporting Countries (OPEC)—have oil for export greater than Unocal's entire US production. Six more could be called upon to make up for a large fraction of Unocal's US output. With US oil consumption at 20.7 million barrels per day in 2005, 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 US balance of payments in

6. Compare Congressional Steel Caucus, letter to Secretary Timothy Geithner, July 2, 2010 with Stan Abram, "The Curious Case of Anshan Steel and the Space-Age Rebar Technology," *Forbes*, July 7, 2010.

7. Press statements on CNOOC's proposed acquisition of Unocal by Representative Joe Barton (R-TX) and Representative Duncan Hunter (R-CA).

© Peterson Institute for International Economics | www.piie.com

energy unchanged. US courts could force CNOOC to pay the switching costs if contracts were broken.

It is commonplace to conclude that the United States needs 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. But the idea that policy toward CNOOC's acquisition would have affected US national energy interests, negatively or positively, does not survive rigorous scrutiny.

Protection of US interests derives from the dispersed structure and fungible qualities of the international oil industry. US oil from the Gulf of Mexico could be used to provision the Chinese People's Liberation Army (PLA) if the US government did not legally or physically block such shipments. But this would penalize the PLA by forcing it to buy expensive oil from North America compared with purchasing it from commercial suppliers closer to home. If CFIUS strategists could be permitted to enjoy a slyly mischievous sense of humor, CFIUS might have required a CNOOC-owned Unocal to ship all its North American output back to supply Chinese military forces. Moreover, in a bilateral crisis, perhaps over a confrontation across the Taiwan Strait, a CNOOC-owned US-based Unocal would be 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 to play, helping to offset countervailing Chinese pressures over US investors on the Chinese mainland.

Might the sale of Unocal to CNOOC have represented a leakage or loss of technology that could damage the United States (Threat II)? Looking strictly at oil production technology—possible enhancement of Chinese anti-submarine warfare (ASW) capabilities is considered below—the answer is no. If incorporating Unocal's technology and managerial expertise into CNOOC would have enhanced the latter's performance in discovering and producing oil, the result would have eased pressure on world energy markets. The spread of Unocal expertise throughout CNOOC would likely have had a small but positive global supply effect. If Unocal engineers and managers had improved CNOOC performance more than they might improve Chevron performance—Chevron ultimately acquired Unocal after CNOOC withdrew—the result would have been a net benefit for US and global energy consumers. On the demand side, the Chinese thirst for oil is a challenge that the entire world has to cope with. On the supply side, the Chinese drive to develop new energy sources is part of the solution, not part of the problem.[8] What serves US national interests can be illustrated with a hypothetical question: If China's government 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

8. For an empirical assessment of whether Chinese investments are "locking up" world natural resources, or—in contrast—are serving to diversify and make more competitive the world natural resource base, see Moran (2010).

© Peterson Institute for International Economics | www.piie.com

executive director vote yes or no? The answer is clearly yes, as it would 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, that operates the only rare-earth mine located in the United States, at Mountain Pass, California. All US government stocks of rare earths in the National Defense Stockpile were sold off in 1998. In 2003 Molycorp ceased mining production at Mountain Pass, but the property remained open on a care-and-maintenance basis. Rare-earth supplies have become a matter of concern since 2009 as China has restricted exports and manipulated supply to show displeasure in foreign policy disputes with Japan. A thorough CFIUS analysis today would consider whether Molycorp should be included in the proposed CNOOC acquisition of Unocal or sold off to an American buyer separately.

Regarding potential leakage of sensitive technology, assertions were made that Unocal seismic technology had dual-use possibilities, reinforcing Chinese ASW capabilities as well as enhancing oil exploration. Investigating these assertions would involve highly specialized, and perhaps highly classified, expertise. Once again, however, the algorithm to be followed would take the form of what has been laid out above: Would acquiring Unocal's seismic technology confer capabilities that are closely held and not available for purchase or hire by China from other alternative sources?

Huawei, Bain Capital, and 3Com[9]

In late 2007 Bain Capital proposed to acquire 3Com, a leading US hardware and software network company based near Boston, for $2.2 billion, with 16.5 percent minority shareholding by Huawei, including the right to appoint 3 of 11 board members.[10] Huawei was founded in 1988 by a former Chinese army officer, Ren Zhengfei. In 2005 the Rand Corporation reported that Huawei had ties with the Chinese government, in particular the People's Liberation Army (PLA) (Medeiros et al. 2005). The DOD 2008 annual report to Congress on the military power of the People's Republic of China named Huawei, along with Datang and Zhongxing, as working 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 had larger market penetration in Europe than in the

9. For detailed background on Huawei, see Barfield (2011).

10. 3Com Corporation, Proxy Statement Pursuant to Section 14(a) of the Securities Exchange Act of 1934. Washington, DC: United States Securities and Exchange Commission, January 24, 2008.

© Peterson Institute for International Economics | www.piie.com

United States and could use a stake in 3Com to provide channels into the US market quite independent of any interest in 3Com products or services.

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.[11] How might this acquisition have posed a national security risk to the United States? This case provides particular insight into the interaction between Threats II and III. The roster of 3Com products suggested as many as nine clusters of goods and services that might be considered crucial to the functioning of the US economy and defense industrial base and that might provide important capabilities to the Chinese economy and defense industrial base, including routers, switches, interface cards, and—most important—network security systems. These needed to be subjected to the concentration-level and switching-cost tests discussed above.

Addressing Threat I first, 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 Huawei minority interest would be enough to allow Chinese interests, or the Chinese government, to dictate how 3Com goods and services were offered for sale in the market. A large fraction of 3Com products are assembled in the wholly owned H3C affiliate and shipped from China; China could embargo them, along with other output that companies such as Cisco or Ericsson produce or assemble on the mainland. But the Huawei ownership share in 3Com would not per se enhance the options available to the Chinese government one way or another.

Turning to Threat II, would 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? The CFIUS threat assessment would likely have discerned for each of the nine 3Com 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 router, switch, and internet card capabilities of 3Com products are rather widely available commercially for Chinese use, many involving hardware and software already produced in China. A focus of particular attention, however, was 3Com's prize-winning integrated security and intrusion-protection system, called Tipping Point, that featured US government and military agencies among its purchasers. Tipping Point 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 a Tipping Point–like threat suppression engine? A review of commercial sources suggests at least 12 US players in this market, including Cisco Systems, Juniper Networks, Sourcefire, IBM, McAfee, Top Layer Networks, Radware, NFR Security, Reflex

11. Bill Gertz, "Intelligence Report Hits China Deal," *Washington Times,* November 30, 2007, A1.

© Peterson Institute for International Economics | www.piie.com

Security, DeepNines, Still Secure, and NitroSecurity, plus European and Asian firms. Specialized expertise would be required to compare the individual attributes of these alternative security systems, but it would appear that Chinese agencies have redundant access to capabilities similar to those of Tipping Point. After some initial reluctance, 3Com and Bain announced that they were prepared to spin off the Tipping Point operations.

Regarding Threat III, the 3Com case introduced an apprehension that has plagued Huawei ever since: that the acquisition might allow for infiltration, surveillance, or sabotage of 3Com's goods and services—or, as a special case of Threat III, that the proposed acquisition might provide insight into weak points of a system that even purchasers and users, including the US government, might not be fully aware of. On March 19, 2008, Bain announced that it was withdrawing its proposal to acquire 3Com. Two years later Hewlett Packard bought 3Com and began to see products in the United States from 3Com's Chinese facilities, an observation that will receive more detailed analysis later in this chapter.

In 2010 Huawei purchased the patent portfolio of 3Leaf, a near-bankrupt Silicon Valley company that had no other bidder on its assets, and hired some of its staff. Only after it discovered CFIUS was investigating the acquisition did Huawei file official notice. Two months later CFIUS informed Huawei that it would recommend to the president that the company divest itself of all 3Leaf assets. In reaction, Huawei issued an open letter defending its reputation and inviting US government agencies to investigate the company. In the end, the company accepted the divestiture, agreeing to appoint an officer whose responsibility was to show US agencies periodically that the company was in compliance.

Apprehension about infiltration, surveillance, and sabotage via Huawei information technology (IT) goods and services extends beyond acquisitions of US companies over which CFIUS has jurisdiction. Huawei was a leading bidder on an AT&T plan to upgrade the US network to operate with 4G technology in 2009, only to find that the head of the National Security Agency (NSA) told AT&T that Huawei must be excluded from consideration if AT&T wanted to maintain its government contracts. In 2010, as Huawei appeared set to win major network upgrade business from Spring Nextel, the secretary of commerce placed a personal call to Sprint's CEO to warn that Sprint's relationship with government agencies would be imperiled if it chose Huawei as a service provider. The instinct to exclude Chinese companies extends beyond mergers and acquisitions over which CFIUS has authority to government contracts, private contracts, joint ventures, and R&D partnerships.

In an attempt to assuage ongoing concerns about Threat III—whether through acquisition of a company or through commercial provision of goods and services—Huawei has established a security assurance program in which the company offers all source code in escrow to a trusted third party that can verify that goods and services are clean to buyers or governments. The most advanced instance of such vetting is Huawei's Cyber Security Evaluation Center at Basingstoke in the United Kingdom, staffed by Huawei employees

© Peterson Institute for International Economics | www.piie.com

who are UK nationals with UK government security clearances. Forensic audits of Huawei hardware and software take place according to UK government parameters and the results are shared with UK intelligence and other agencies, which are expected to share information with counterparts in the United States, Australia, Canada, and elsewhere. Complementing this audit of hardware and software is the proposal that indigenous trusted third-party installers, such as Bechtel, CDTI, or TESSCO, take goods and services that have been verified as secure and deliver, install, maintain, and manage upgrades and updates for purchasers. No Huawei individual or entity thus touches Huawei goods or services between the security audit and the installation or upgrade with final users.

The security assurance arrangement may provide a model that extends far beyond concerns about foreign acquisitions of local companies. As cyber-security experts such as James Mulvenon and James Lewis point out, global supply chains that supply IT infrastructure are pervasive, containing hardware and software that come from China, Russia, Malaysia, Mexico, and Eastern Europe.[12] Cisco, Ericsson, Lucent-Alcatel, Samsung, and other international IT firms source goods and software from Chinese facilities staffed by Chinese engineers often within sight of Huawei facilities. Scott Charney, corporate vice president of trustworthy computing at Microsoft, argues that cyber security cannot be achieved by trying to single out firms of a particular nationality or firms with production in a particular country (Charney 2008). On the second Tuesday of each month, he reports, Microsoft applies patches and upgrades to many millions of computers in China, including those of the PLA. "China and other governments have expressed concerns about back doors in US products," notes Charney.[13] "When asked about this, I have stated numerous times that Microsoft does not put back doors into its products. Indeed, if we did, it would undoubtedly be discovered and then we would be out of business." National and international efforts to deal with cyber intrusion will have to address purchases of hardware, software, installations, upgrades, and patches from providers of all nationalities operating from all locations. Protection from threats may require an array of independent cyber security cells around the globe that vet the hardware and software of all major IT providers, providing assessments to private clients and governments alike—a vast subject well beyond the scope of this volume.

Tightening CFIUS Appraisal of Potential National Security Threats from Proposed Foreign Acquisitions

Each of the three threats described above can be found in the language of Section 721 of the Defense Production Act of 1950 and subsequent amendments,

12. This cyber-security appraisal draws upon Barfield (2011).

13. Personal communication on December 18, 2011.

© Peterson Institute for International Economics | www.piie.com

including FINSA.[14] But the language fails to adequately guide an analysis to identify realistic national security threats or set aside implausible national security preoccupations.

Concern about Threat I (denial) is expressed, among other places, in consideration of whether the 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."[15] But the concept of control is not operationalized to mean that the acquirer could delay, deny, or place conditions upon providing a good or service to adversely affect US national security. For this to be possible, as argued above, the number of suppliers must be concentrated, the number of close substitutes limited, and switching costs high. Otherwise Lenovo's purchase of IBM's computer business might be considered a shift of control to China—true enough—even as Lenovo's PCs are so generic that hypothetical Chinese government instructions to withhold PC sales to US buyers would have no perceptible effect on US national security.

Concern about Threat II (leakage) is expressed, among other places, in consideration of the potential effects of the transaction on transfer of military capabilities: "the potential effects of the transaction on sales of military goods, equipment, or technology."[16] But the worry about leakage is not qualified by consideration of whether alternative sources of military goods, equipment, or technology are readily available to a country or not. When sources of supply are so diverse that there are off-the-shelf commercial substitutes for the goods and services that a target of foreign acquisition provides, there is no basis for determining that an acquisition might open a channel for leakage of goods, equipment, or technology.

Concern about Threat III (sabotage, espionage) is expressed, among other places, insofar as "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."[17] As argued earlier, CFIUS-FINSA language might be amplified to include infiltration and surveillance, plus detection of network weaknesses and possible internal system manipulation. But the broader issue for the United States and other states worried about cyber security is how to protect against potentially infected goods and services by screening them

14. US Department of the Treasury, Committee on Foreign Investment in the United States (CFIUS), Section 721 of the Defense Production Act of 1950, Final Regulations, Issued November 14, 2008, www.treas.gov (accessed on October 30, 2011).

15. FINSA, Section 2, (a), (3), (4).

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

17. FINSA, Section 2, (a), (5), (6).

© Peterson Institute for International Economics | www.piie.com

wherever they come from and through whatever channel they are purchased, a challenge in which foreign acquisitions per se are only a subset.

CFIUS members and staff, intelligence community support, and Congressional overseers should generally be able to find adequate justification in current legislation and regulations to deal with the three threats identified here. But they are left without appropriate filters to discern truly troublesome cases from harmless ones. Much more problematic for the review process, the legal language involving "critical" and "essential" are introduced without qualification, leaving great potential for protectionist mischief. For example, "the term 'critical technologies' means critical technology, critical components, or critical technology items essential to national defense."[18] Foreign acquisition of a US steel producer, as in the Oregon steel case, would certainly involve a "critical" and "essential" item of importance to national defense, leading the reader of FINSA, Section 2, (a), (7) possibly to consider the acquisition a national security threat. There is no guidance to point out that the multiplicity and diversity of alternative steel suppliers would render any attempt to delay, deny, or place conditions on access of supply to be entirely useless, and any transfer of technology to be 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 be kept in the hands of home-country citizens.

The approach recommended here for CFIUS assessments can readily be generalized for multilateral use among developed and developing states. Looking first at more developed countries, the Three Threats framework fits comfortably within the Guidelines for Recipient Country Investment Policies Relating to National Security, a set of recommendations the Organization for Economic Cooperation and Development (OECD) Council adopted in May 2009, while suggesting a decision tree for OECD members to evaluate the plausibility of actual national security threats. The utility of the framework does not rely on agreement among the community of nations as to which countries might be considered "good" or "bad" states (or "hostile" or "rogue" or "unreliable"). Rather, the framework is constructed with a realpolitik assessment that governments have different and sometimes seriously conflicting conceptions of their own national interests, allowing national authorities to ponder carefully whether a foreign acquisition credibly poses any of the three threats identified here. The fundamental value of the framework is to separate plausible from implausible threats in a manner that all nations might commonly accept. That is, individual states could base their own behavior around the framework, recognizing that they can live comfortably within a global regime in which others behave in a similar fashion.

When is blocking foreign acquisitions pure protectionism? The framework offered here does not attempt to second-guess the specific motives for any given rejection of a proposed foreign acquisition; rather, the intention is to offer a

18. FINSA, Section 2, (a), (7).

© Peterson Institute for International Economics | www.piie.com

rigorous line of reasoning to identify credible threats. There will always be close calls along the margin. But US experience suggests that public officials need a decision tree to help them determine when high-profile contentions are simply bogus, often fueled at least in part by acquisition-minded US competitors.

The framework introduced here complements and enhances the goals of transparency of policies, predictability of outcomes, measures of general application that treat similarly situated investors in a similar fashion, proportionality of measures, and accountability of implementing authorities as set forth in OECD guidelines for recipient country investment related to national security. It advances the guidelines' purposes in two ways. First, the OECD guidelines permit that "essential security concerns are self-judging"; that is, "OECD investment instruments recognize that each country has a right to determine what is necessary to protect its national security." The decision tree in figure 4.1 offers a common path for all OECD members to evaluate whether concerns about a possible national security threat are plausible. Second, the OECD Investment Committee occasionally uses the term "strategic industries" in ways that suggest entire sectors—energy, military suppliers, financial institutions, infrastructure—might be excluded from foreign takeovers. The threat assessment tool developed here allows for finer discrimination as to when a proposed foreign acquisition might pose a threat.

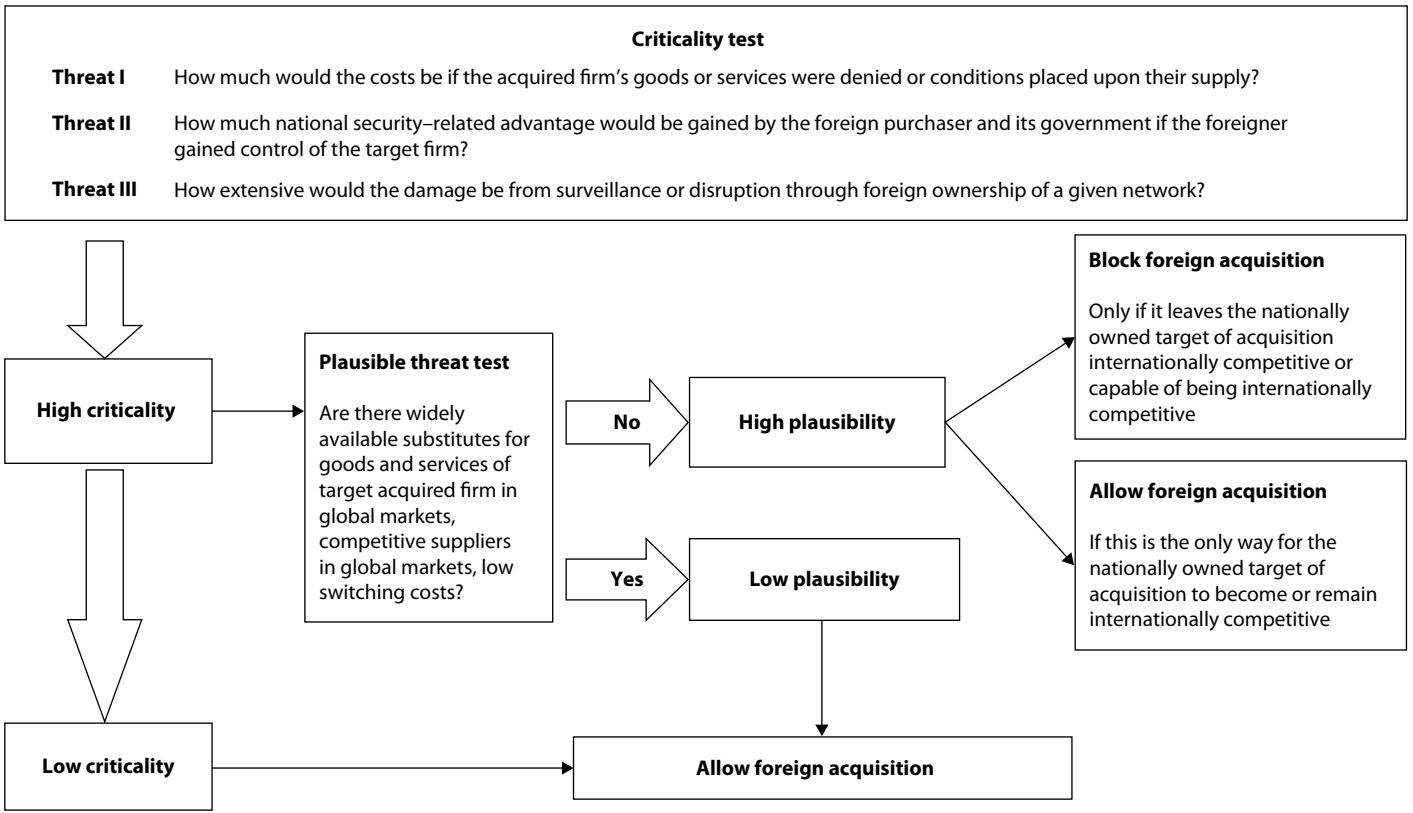
Use of the decision tree need not be limited to OECD members. It can equally well form the basis for non-OECD nations, such as Brazil, Russia, India, or China. In assessing the degree of competition among suppliers and switching costs, it is important to focus on the global market, not the domestic market; the relevant measurement is whether an acquisition increases the concentration in the global market to a worrisome extent, not whether the acquired firm is the last producer on home-country soil. There will be many instances in which a foreign company may acquire the last remaining national producer of a given good or service, but the international market is sufficiently competitive that it makes no substantive difference for the home country's national security.

Can a quantitative standard be used to guide an OECD-wide, or worldwide, plausible threat test—that is, to determine whether there are "widely available substitutes for goods and services of the target acquired firm in global markets, competitive suppliers in global markets, [and] low switching costs"? The most obvious tool to operationalize the degree of competition among suppliers is to use the long-standing US Department of Justice and Federal Trade Commission—or similar EU Directorate General for Competition—guidelines on mergers and acquisitions.[19] The goal is not to turn the national

19. US Department of Justice/Federal Trade Commission, "Commentary on the Horizontal Merger Guidelines," March 2006, www.usdoj.gov/atr/public/guidelines/215247.htm (accessed on December 20, 2012); European Union, European Commission's Directorate-General for Competition (EU DG Competition), January 2008, http://ec.europa.eu/atoz_en.htm (accessed on December 20, 2012).

© Peterson Institute for International Economics | www.piie.com

Figure 4.1 Decision tree to assess national security rationale for blocking foreign acquisition



© Peterson Institute for International Economics | www.piie.com

security framework into an antitrust issue, but to limit national security scrutiny to circumstances in which denial of access to an acquired firm's goods or services would impose high costs, or in which the unwanted advantage to the foreign purchaser and its government would be large, or in which damage from surveillance or disruption through foreign ownership of a supplier would be unavoidable. In each case, national security monitors would want to look for consequences that affected the home country in ways far beyond raising prices.

© Peterson Institute for International Economics | www.piie.com