
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.

