SKATING ON STILTS

Why We Aren't Stopping Tomorrow's Terrorism

Stewart A. Baker

HOOVER INSTITUTION PRESS
Stanford University Stanford, California

11 Invested in Insecurity

The city of Dubai leaps straight out of the flat sands and flat seas of the Arabian Peninsula. One minute you're driving through scrubless desert, the next you're cruising an elevated freeway past a phalanx of thirty-story skyscrapers, most built in the last ten years. Today, with a mountain of debt, Dubai has the look of last year's boomtown; the newest skyscrapers lack tenants and construction has nearly ceased. But during its heyday from 2005 to 2009, Dubai's ambition seemed as unbounded as the desert that it sprang from. And part of its plan was to become the great transshipment port of the Middle East—just as Singapore is the great entrepôt of the Far East. By 2006, with several bustling modern ports, it had largely succeeded.

That's when it encountered—and transformed—the Committee on Foreign Investment in the United States, first handing DHS its best tool for combating network security threats and, eventually, taking that tool out of the department's hands.

The success of the port of Dubai was due in no small part to Dubai Port World, a company owned by the royal family. DPW, as it was called, was the principal terminal operator in Dubai. Its success there led it to branch out, purchasing terminals in many other ports.

Running a port is a lot like running a small city. The government usually provides police, fire protection, and perhaps utilities, while the terminal operators carry out the main economic activity—storing goods and moving them from ship to land and back. To do that, the terminal operator leases land in a port and then builds a pier for ships, cranes to unload the ships, a parking lot for the cargo to rest, plus

perhaps a small management office. The operator makes its money lifting containers out of ships and holding them for shippers to pick up. The terminal operator is thus a lot like a store owner in a city—economically vital but responsible mainly for his own property.

Operating a terminal was once a local business, just like a store. But globalization has come to the industry, and the top five operators in the world now handle more than a quarter of all trade. None of the biggest operators is an American company; in fact, even in the United States, four out of five terminals are operated by foreign companies.

So it didn't exactly set off alarms when one of these foreign terminal operators decided to buy another foreign terminal operator.

Soon we would wish that it had.

The buyer was DPW. The seller was P&O—the Peninsular and Oriental Steam Navigation Company, a two-hundred-year-old British firm that also had terminal operations in much of the world, including the United States. P&O leased terminals in six U.S. ports, and DPW would be getting those along with the rest of the company.

DPW asked the Committee on Foreign Investment in the United States, or CFIUS, to approve the transaction. Created by executive order in 1975, CFIUS conducts national security reviews of foreign investments in U.S. companies. As long as we are running fiscal and balance of payments deficits, the United States pretty much has to keep selling many of its assets to foreign buyers. But we also have to fence off some companies and sectors for national security reasons. We would not let an adversary—Iran or North Korea, say—purchase a major defense contractor. The opportunities for espionage and sabotage are too tempting. But defense contractors are not the only companies that create opportunities for espionage and sabotage. We would not want, say, major U.S. telephone companies to fall into the hands of countries that might use the companies to spy on Americans.

At bottom, CFIUS was charged with deciding which transactions posed unacceptable national security risks. The committee has broad but vague powers. In essence, any foreign company buying a

U.S. company has the option of notifying CFIUS of the transaction. If CFIUS doesn't do anything within thirty days, then the transaction can go forward. If CFIUS has questions, it can launch an investigation. In theory, the investigation is completed in forty-five days and a recommendation is made to the president, who has fifteen days to decide whether to block the transaction on national security grounds.

That's the theory. When Congress first set rules for CFIUS in 1988, it imagined a fairly quick ninety-day process with a sharp yes-or-no decision at the end. Congress took pains to avoid delaying investments. In addition to the short decision deadlines, Congress allowed companies to skip the CFIUS process completely.

Why do companies go through the CFIUS process if they don't have to? It's simple; they want certainty. If they notify a transaction to CFIUS and get no objection, then the United States can't overturn the deal later on national security grounds (unless the information supplied by the parties was false or misleading). So if the parties to a transaction have even a tiny concern about whether the deal will raise national security objections, it's a good idea to make a CFIUS filing. Most investors want to find out about national security objections early, when the deal can still be unwound. If the concerns arise later, one party or the other may be hurt badly. It's almost impossible to unscramble the eggs once a deal has been finalized, and the effort to do so would put both companies at risk.

When we were at DHS, we estimated that only about 10 percent of large transactions received CFIUS review. The rest didn't raise even modest national security concerns. Of that 10 percent, the vast majority were approved without comment. Only about 10 percent of submitted cases led to further action by the committee, meaning that the committee devotes almost all of its attention to roughly 1 percent of all the investments made by foreigners in U.S. companies.

But the stakes for that 1 percent can be enormous. Congress gave the president authority to block any foreign acquisition of a U.S. company if the committee found credible evidence of a threat to national security.

Whether to seek CFIUS approval for the Dubai Port World transaction must have been a close question. Neither company was based in the United States, after all. But CFIUS still could exercise some authority over the transaction. Six U.S. terminals would be getting a new foreign owner.

At the same time, asking for approval didn't look like a big risk. No one in CFIUS had ever raised a national security concern about the ownership of terminals in U.S. ports. And the banks that back these transactions are notoriously risk-averse; if there were a CFIUS issue, they'd want to know right away, not after the deal was done. So DPW decided to go for the certainty of a committee approval. Since DHS was the recognized expert in port security and one of the toughest security advocates on the committee, DPW consulted us early.

I had just taken over as head of policy, and CFIUS had just been assigned to my office. I had no staff of my own, but I wasn't a stranger to CFIUS. After leaving NSA, I had many clients with CFIUS concerns, and I had negotiated some of the detailed agreements that the Justice and Defense departments insisted upon when foreign companies acquired large interests in U.S. telecommunications companies. I knew how valuable CFIUS could be in protecting security, and I was pleased that DHS had already established itself as a leader on the committee.

While the Defense Department had long worried about foreign investments involving its contractors and its technology, its main concern was military threats to our security. But on 9/11 al Qaeda had used civilian technology to kill more Americans at home than any foreign military attack had ever done. So from the start, DHS focused on ways in which foreign ownership might expose the home front to unconventional attacks. Because national security was not defined narrowly, DHS had no trouble fitting this approach into the statute, and in 2007, Congress ratified DHS's approach by explicitly including homeland security and critical infrastructure protection in the new definition of national security.

DHS's broad view of national security covered a lot of ground. But our top worry was sabotage and espionage in the information technology sector. We knew that there were some governments that routinely asked their companies to help spy on other countries. And any technology that allowed spying could be used for sabotage. Once a hostile nation has compromised a computer, it is up to that nation whether to exploit the computer or shut it down. That was too big a risk to take, DHS argued. Some companies and some countries just couldn't be trusted. They shouldn't be allowed to control U.S. networks.

The federal government doesn't have authority to set cybersecurity standards generally for the private sector. It doesn't even have authority to exclude from U.S. markets companies and products that are likely to be used for espionage. It can prosecute spies and companies that conspire with them, of course, but only after the damage is done, and a successful prosecution depends on compiling proof beyond a reasonable doubt and, often, on extradition or other cooperation from the government that ordered the spying. It's not much of a weapon.

CFIUS, however, offers real authority to protect telecom and IT security, and DHS moved quickly to ensure it was used for that purpose. When a company or country with a questionable reputation filed to acquire a U.S. IT or telecom company, DHS often asked the intelligence community whether either had engaged in espionage against the United States or others. (This practice was eventually institutionalized for all applicants.) Even if the company or country hadn't actually been caught in the act, DHS would assess whether the transaction increased U.S. vulnerability to the kind of cyberattacks we knew were likely in the long run.

A number of transactions did increase U.S. vulnerability. The telecom industry is globalizing at the same time that it is shifting from big, specialized telephone switches to Internet technologies. The IT industry has been globalized for decades, but opportunities to compromise components and complete products continue to grow, particularly as companies diversify their software as well as their hardware supply chains. DHS paid special attention to foreign investment in

computer security products and services. Just as terrorists hoping to assassinate an official are most likely to succeed if they can gain control of the official's security detail, so attackers hoping to compromise a network are most likely to succeed if they can gain control of the network's security system.

The terminal deal that DPW was proposing, though, had nothing in common with the transactions that most threatened U.S. interests. In telecommunications and information technology transactions, we knew there was a risk that foreign buyers might use their new acquisition as a base for espionage or network attacks. But why would Dubai want to sabotage a U.S. port? And even if it did, how would owning a terminal make that more likely?

The terminals that DPW was buying were just plots of land and warehouses inside six U.S. ports. Their security was overseen by the port authorities, the local governments, and the Coast Guard.

I polled the DHS components responsible for ports and found no concerns about the transaction; they all said that the current owner cooperated fully and voluntarily in all our security programs, and they had no reason to think that DPW would act differently. None of the other CFIUS agencies took even a passing interest in the deal.

Even so, there was one more thing we could do. I knew that companies had entered into "mitigation agreements" with CFIUS agencies in the past. In fact, I'd negotiated them. Could we get one here, I wondered?

Mitigation agreements weren't anything that Congress had created. When Senator J. James Exon and Representative James Florio drafted the Exon-Florio Amendment[1], they expected CFIUS to ask a straightforward question about a foreign takeover: "Will this transaction put national security at risk?" And the answer, they thought, would be binary: either yes or no.

In the world of real transactions, though, it is rarely that simple. Suppose a company we don't fully trust wants to buy a company that sells software. Most of the software is plain vanilla consumer

stuff—spreadsheets, word processing programs, and the like. But one of the products is a centrally managed security service that screens all the packets that flow in and out of the user's computer. We might be able to live with the risk of compromise to the consumer products, but if the security service is ever compromised, every user's machine will be owned by a foreign intelligence agency from the day they install the software. That's too great a risk. We decide to oppose the transaction.

When it learns of our objection, though, the buyer says something that neither Senator Exon nor Representative Florio expected.

"Actually, we aren't interested in the security service. We've been planning to sell it. Can you approve the deal if we spin it off?" the buyer asks.

The sensible thing is to agree. We'll get everything we want without blocking the deal.

But what if there really isn't time to sell the security company before the CFIUS statute requires us to say yes or no to the transaction? We have only thirty days, after all.

"Well, will you approve the deal today if we *promise* to sell the subsidiary as soon as possible?" the buyer asks next.

Again, the sensible thing is to agree, as long as we know the buyer's promise will be kept. But to make sure it is, we need a strict agreement that can be enforced long after the transaction has been approved.

That simple example shows why CFIUS found itself forced to invent what became known as a "mitigation agreement." If the buyer entered into a binding agreement that mitigated any security risk in the transaction, the committee would approve the deal. It was good for everyone. The buyer and seller got what they wanted. And so did CFIUS—in fact, it got what it wanted without saying no to a foreign investment, something that can give a country a bad name in investment circles.

But a mitigation agreement doesn't have to be limited to something as clear-cut as the sale of a subsidiary. Sometimes the buyer wants to keep a subsidiary but has no interest in running it. It may solve a security

concern by promising to leave the current American management in place. Before CFIUS can rely on that promise, though, the company has to put it in writing and agree to be legally bound by it.

DPW had been telling us it had no interest in changing the management or practices of the U.S. terminals. I decided that we would ask DPW to put that in writing. After all, there was at least a small risk that the new owners would want to reduce costs by cutting security. A mitigation agreement would lock them in to their promises.

It turned out to be an easy sell. DPW agreed that it would stay in the voluntary security programs that P&O had joined. For good measure, DPW agreed to an open-book arrangement with DHS, allowing the department to inspect its records and obtain employee security data at will. These were incremental improvements in security, and DPW was willing to provide them in order to smooth the way for the transaction.

DHS did not need to get the approval of CFIUS to negotiate these provisions; we were the only agency on the committee with the slightest interest in this transaction. Once DHS was satisfied, the rest of the committee quickly okayed it.

By mid-January, CFIUS had finished its thirty-day review, DPW and DHS had signed the mitigation agreement, and the deal had cleared. According to the law, DPW was fully protected by the safe harbor provision of CFIUS. The United States could not legally overturn the deal.

A week went by, then another. Although CFIUS approval was in place, DPW was still in a bidding war with another purchaser. Not until February 11, when its rival bowed out, was DPW's victory announced in the business press. The contest was over.

Or, rather, it would have been but for a small company in Miami. Eller & Company had two joint ventures with P&O. For some reason, Eller didn't want DPW to take over that relationship. So it hired Joe Muldoon, a retired lobbyist and polo player, to get the deal overturned somehow. In the end, Muldoon turned out to be one of the

great overachievers in history. Not since Andrew Jackson fought the Battle of New Orleans has anyone won such an influential victory after the war was over. And never has such a public fuss been unleashed on behalf of such a tiny commercial interest.

Muldoon had never handled a CFIUS matter, and he probably didn't know that the approval was already final. He also didn't know—or perhaps didn't care—that terminal operators don't have much to do with port security. He just started telling anyone who would listen that national security was somehow at stake in the transaction. Finally, two weeks after the deal had been approved, someone heard him.

On Sunday, February 12, a story by the Associated Press claimed for the first time that the deal raised security issues, a twist raised by Senator Charles E. Schumer, who said that the transaction would "outsource . . . sensitive Homeland Security duties."

I assumed he was repeating things he heard from Muldoon. They weren't true.

But that didn't matter.

By the end of Sunday, the blogs were buzzing. And the administration's rapid response team was silent. For one good reason. They had no idea what Senator Schumer was talking about. The transaction had set off no alarms as it wended its slow way through CFIUS. The lobbyist and politicians now complaining had said nothing while the deal was being reviewed.

And the review process had been over and done with for a month. For policymakers, that might as well have been eternity. Whatever whisper of worry they might have heard at the time of approval had long ago been crowded out by more pressing matters. Not until the working staff who had dealt with the case came to work on Monday were we able to gather the information we needed to respond.

By then it was too late. On Tuesday, February 14, the press had launched a story line that treated the transaction as the sale—lock, stock, and barrel—of six large American ports to an Arab company. That was the line taken that day by the Associated Press, which headlined the story "Arab firm may run 6 U.S. ports."[2] Soon, the *Washington*

Times had the same slant: "Some of the country's busiest ports—New York, New Jersey, Baltimore and three others—are about to become the property of the United Arab Emirates."[3] By Friday morning, a *Washington Post* writer channeling administration critics was frothing: "The management of major U.S. ports taken over by an Arab-owned company? What was the Bush administration thinking when it allowed such a thing?"[4]

For a couple of weeks, that was the nicest thing anyone said about us. No one listened when we tried to explain that port security is the job of the port authority and DHS, not the terminal operators.

It was a full-fledged Washington panic, of a kind seen only rarely, when a brand-new issue breaks suddenly and politicians have to wing it, with only their jangling switchboards for guidance.

The talk shows and blogs had a field day. So did the partisans. The issue let Democrats get to the president's right on national security by demanding that Arabs not be allowed to run the security of American ports. Congressional Republicans, who couldn't afford to seem soft on national security, rushed to condemn the deal as well. Congressmen of both parties launched crude attacks on Dubai and the United Arab Emirates to which it belongs. Congress held hearing after hearing to condemn the administration and to demand that the deal be overturned. In the end, the company buckled, promising to sell off its U.S. port properties.

A Washington panic is a funny thing. It seems to take Washington by the throat. No one can think or talk about anything else. Congress is suddenly ready to enact legislation in days, not weeks or months.

And then, like a tropical monsoon, the panic lifts. The clouds part. Politicians blink a bit shamefacedly in the sun. And everything goes back to normal.

That's what eventually happened with the DPW case. Though you couldn't have guessed from the hearings, our message slowly got through: DPW wasn't buying American ports, we patiently repeated. It wasn't going to be responsible for security. It had signed an unprecedented

mitigation agreement that addressed any reasonable security concerns. And Congress's noisy performance was undermining the U.S. reputation as a good place to invest—as well as CFIUS's reputation for raising only serious national security concerns.

Behind the bluster, Congress started to get nervous. It began looking for an exit. When DPW finally bowed to political reality and agreed to get rid of P&O's U.S. facilities, Congress was eager to claim the scalp and move on. Muldoon had earned his fee, at great cost to America's credibility in world financial markets.

The monsoon had passed. The sun was out again. But the DPW affair would hang over CFIUS for the rest of President Bush's second term. For a time, fear of another CFIUS eruption would allow DHS to turn the committee into a powerful bulwark against new computer and telecommunications insecurities. In the end, though, it would create a business backlash that showed the limits of security regulation even in a time of great and growing vulnerability.

For DHS, the fight over Dubai ports was a distraction from the real security risks posed by globalization of telecommunications and networks. The insecurity of U.S. networks wasn't just an organized crime problem. It was the result of deliberate policies adopted by countries that viewed us as an intelligence target. If they could get their companies to compromise U.S. networks, they'd do it in a heartbeat. So allowing foreign companies to take up critical positions in U.S. computer and telecommunications networks, either as suppliers or as service providers, raised serious national security issues. At the same time, globalization was relentless. The old days, when AT&T provided local and long distance service—and made all the equipment on the network—were long gone. And the collapse of the high-tech bubble had transformed the industry that emerged from AT&T's breakup. The Baby Bells were consolidating; long distance was disappearing as a separate business; wireless was displacing land-lines; and the equipment companies that had dominated North America for a century were in trouble. We couldn't just say no when foreign companies came

courting. In that context, mitigation agreements became a way to say yes to globalization without completely surrendering to foreign espionage. The agreements became a kind of company-specific network security regulation. We began to insist on a mitigation agreement in any transaction that posed even a modest threat. Each agreement created an ad hoc regime designed to curb foreign government infiltration of U.S. telecommunications and information technology.

The toughest agreements created a wall between the foreign owner and U.S. production facilities. This was common where CFIUS wanted to approve a deal in which the acquired company had sensitive government contracts. The wall was meant to keep the contracts free from foreign influence. The same thing was occasionally done for highly sensitive commercial contracts.

Another common security measure was to insist that the government (or an approved third party with technical skills) be guaranteed the right to inspect the buyer's hardware designs and processes, its software source code and testing results, and any other part of the production process that might reveal a deliberate compromise. To make sure that data was not shipped abroad and compromised there, some mitigation agreements required that data about Americans be kept in the country; sometimes the agreements required special security measures for the data.

The agreements also established a host of procedural security safeguards. These often included a government-approved security officer with broad powers and an obligation to report any suspicious incidents to the U.S. government. They also included regular audits by the government or a third party designated by the government. Personnel with access to sensitive data typically had to be screened; this sometimes included limits on outsourcing. Workers usually had to be trained in the security requirements and encouraged to report violations; and whistleblowers had to be protected from retaliation.

We were acutely aware that these measures weren't perfect. The substantive requirements were at best a mixed bag as far as security went. In theory, access to source code and hardware designs would

allow our experts to find any Trojan horse built into the product. But few government workers have the expertise to find these needles in a haystack of products. Unless we insisted that the companies pay for very expensive outside experts to check their work, or we received an intelligence tip about corporate misbehavior, we had only a modest chance of catching a really clever compromise.

The same was true of the procedural safeguards. Reporting obligations and whistleblower protections couldn't guarantee that we'd hear about an attempt at compromising U.S. products. They just increased the chances that someone would blow the whistle.

Still, imperfect as they were, mitigation agreements were well ahead of whatever was in second place. They were in fact our only good tool for policing foreign efforts to build insecurity into U.S. networks.

There was just one difficulty. The law didn't actually authorize mitigation agreements. No one knew how to enforce them, or even whether they could be enforced. If we were going to turn mitigation agreements into a kind of regulatory regime, we'd have to make sure they got the same respect as other regulatory measures.

Practically the first case I saw when I came on board was a small transaction that raised just this concern. The confidentiality of the process prevents me from providing details unless the companies have made them public, so I will not name the foreign buyer or the U.S. target. But both sold computer security products, so trust was critical. If you can't count on the loyalty of the company that provides your security, you have no security. *Quis custodiet ipsos custodes*—who will guard the guards themselves?—and all that.

As it happened, the foreign buyer of the security company had already entered into a mitigation agreement with DHS. An earlier transaction had been flagged for review, but the company had persuaded the government that negotiated safeguards would protect the national interest. The new case was tougher, but it became easier as we looked more closely. It turned out that no one had closely followed up as the company implemented the earlier agreement. The company

had sent the government letters putting forward self-serving interpretations of the agreement, and no one in government had responded. Now, as we took a close look, we didn't like what we saw. We were sure that the company had deliberately misread—and then violated—the mitigation agreement.

That was that. Why would we trust the company a second time if it hadn't lived up to the first set of promises? DHS took the lead in fighting the transaction. We ruled out another mitigation agreement. The transaction had to be rejected, we insisted. After a long period of disbelief that DHS truly intended to block the deal, the foreign buyer ultimately withdrew from the transaction.

That was the right result. The risk of foreign ownership can hardly be higher than in the area of security services. If we couldn't rely on the company's promises we couldn't find a middle ground.

I knew that the decision would enhance compliance with mitigation agreements. Before this, lawyers could tell their foreign clients that compliance with mitigation agreements was, if not optional, at least negotiable. After all, they might not even be enforceable, and for sure the government would have to sue to get compliance. If so, what was the harm in adopting an unreasonably narrow reading of the agreement? As long as its reading sounds plausible to a judge, the client would suffer no harm from defying the intent of the agreement.

But we didn't want to be forced to go to court over every misreading of the agreement, as though a security agency was just another party with a contract claim. Now we wouldn't have to. We had made it clear that companies would suffer very severe consequences indeed if they failed to live up to a reasonable reading of their mitigation responsibilities. We had taken a big step toward making CFIUS mitigation agreements a credible regulatory regime.

Still, I wasn't completely happy with DHS's performance. Not one member of CFIUS had taken responsibility for making sure the mitigation agreements that protected our security were actually being followed. How could we expect companies to take these mitigation

agreements seriously, I asked, if the government agencies that negotiated them didn't seem to care?

In one sense, DHS was the last agency that should have been responsible for enforcement of mitigation agreements. We were brand-new members of CFIUS, and the Policy office, which had been assigned to handle CFIUS, didn't exist until late 2005 and had not yet been staffed. Even so, we decided to take the lead in reviewing and auditing all of the mitigation agreements that DHS had signed. I hired Stephen Heifetz, a lean, sharp lawyer whose instincts and work habits had been honed in private practice. He could handle anything that the big-firm lawyers on the other side of the table threw at him.

Once he had his team assembled, I sent Heifetz out to audit the companies that had signed mitigation agreements with DHS. The team gave notice that they were coming, but not too much. When they arrived, they demanded records showing compliance and also insisted on reviewing all emails relating to the agreement. If the companies had been deliberately skirting their obligations it would have been hard to hide.

As we expected, most companies were complying, but we also saw clearly that they had become less than vigilant over the years. Heifetz said that email records told the same story in almost every company. Once the deal was done, months might go by without any special attention to the mitigation requirements. Then, suddenly, there would be a spike in high-level attention to compliance. The companies would launch internal reviews to make sure their performance was up to snuff. The spike almost always occurred a day or two after we had sent notice that our audit team was coming out for an inspection.

That was exactly what we hoped to achieve. It is human nature not to follow inconvenient rules when no one is watching. Every regulator knows that. If you want your rules followed, you have to remind companies that you're watching. That's what our audits did. Never again would the companies feel that DHS didn't care whether they complied with mitigation agreements. We were on our way to creating a successful cybersecurity enforcement regime.

This was not our only step to ensure that mitigation agreements were respected. We began to include financial penalties in the agreements. And to make sure that the buyer could never treat fines as simply a cost of doing business, we tied the size of the penalties to the value of the target company. The bigger the transaction, then, the higher the price would be for violating the agreement.

We soon had an opportunity to show we meant business when it came to assessing fines. One buyer of highly sensitive equipment had agreed to spin off a particular portion of the business within a few months of the closing. As the deadline grew nearer, though, the company began coming in regularly, explaining how hard it was working to find a buyer, and how much trouble it had encountered. It was clearly angling for an extension. We agreed, but we also declared that we'd begin imposing fines if the next deadline was missed. What's more, the fines would get bigger every month.

After agreeing to those terms, the company missed the next deadline, too. It asked us to forgo the fines. We refused. The penalties kicked in. As they began to mount, the company quickly found a way to spin off the business.

In a handful of cases, where the national security stakes were very high, we went even further. As the North American equipment market collapsed, the dominant supplier, Lucent, began to hemorrhage. The company put itself up for sale, and Alcatel won the bidding. For us, the stakes could not have been higher.

Alcatel manufactures telecommunications equipment and has been quite close to the French government for years. The French government had frequently been accused of carrying out espionage against U.S. targets. Lucent may have fallen on hard times, but it still manufactured and maintained the switches that carry most of North America's telephone calls. It was the home of the storied Bell Laboratories, whose Nobel-winning research had developed technologies from the transistor and the laser to the Unix operating system. Even the slightest risk that Lucent's capabilities might be turned against the United States was unacceptable.

I thought hard about saying no to the transaction, but the more we looked at the market, the more convinced we became that Lucent couldn't survive on its own. Vetoing the deal would put Lucent on a road to rapid decline. (That judgment still looks correct in hindsight; at the time, Nortel, the other North American telecom manufacturer, looked a bit healthier and chose to stay independent as the industry consolidated. That strategy turned out worse than Lucent's. In 2009, Nortel declared bankruptcy and was sold off in pieces.)

To salvage what we could from a bad set of options, DHS and other national security agencies decided to approve the deal and negotiate the toughest security measures ever imposed under CFIUS. We wanted above all to make sure that there would be no cheating on the deal. To make sure that the agreement would be scrupulously observed, the committee decided on the harshest penalty for breach that had ever been proposed.

If Alcatel breached the agreement in a way that threatened U.S. security, we insisted, the committee could reopen the acquisition. In other words, if there was a breach, the United States could require that Lucent be disgorged and restored to independence. This was called the "evergreen" provision because CFIUS's right to disapprove the transaction would remain in effect forever.

Alcatel and Lucent were nearly slack-jawed when we put this proposal on the table. How could that possibly work, they wanted to know. Five or ten years after the transaction had closed, Lucent would be deeply integrated into Alcatel; undoing the merger at that point could be a death sentence for both companies.

They weren't wrong. No one was sure how the companies could be pried apart at that stage. For that reason, some doubted that the United States would ever invoke the remedy. But the committee members believed that the risk was enormous—a compromise of Lucent's switches could disclose all of the government's wiretaps and make Americans subject to foreign wiretaps at home. If those were the stakes for U.S. national security, we needed to do everything possible to deter a violation of the network security measures.

A death sentence, we thought, should provide a measure of corporate deterrence.

In the end, Alcatel and Lucent accepted the agreement, including the evergreen clause. They decided that the risk created by the clause was material to their future prospects and disclosed it publicly to their investors (which is why I can discuss it publicly). In some ways, the Alcatel-Lucent deal was a high-water mark in the effort to make CFIUS a bulwark against subversion of U.S. information and telecommunications networks. It was public, it was demanding, and it was clearly going to be enforced. Indeed, other agencies, particularly Justice and the Treasury, began imitating DHS and bulking up their audit and enforcement capabilities at about the time we signed the Alcatel-Lucent agreement.

The tough new CFIUS regime benefited from the fallout from the Dubai port debacle. No policymaker wanted to be caught asleep at the switch if another transaction raised national security concerns. Agencies that had shown little interest in CFIUS before DPW now understood its importance, and they were reluctant to second-guess the security agencies. At least at first.

The same was true of investors, who had come to think of CFIUS as something of a paper tiger. CFIUS filings had hit an all-time low in 2003, but by 2006 and 2007 they had rebounded to levels not seen since Exon-Florio was enacted. (Part of that was DHS's doing; we began actively monitoring new transactions and requiring the parties to bring their deals—no matter how small—to CFIUS for review.)

Mitigation agreements also increased. DHS had signed seven such agreements in 2004 and 2005. In 2006 and 2007, after DPW, DHS signed an average of fifteen mitigation agreements a year. And many of the strongest enforcement measures for mitigation agreements were adopted in the same time frame.

For all the value we got from mitigation agreements, we weren't kidding ourselves that we'd solved the cybersecurity problem. CFIUS and its mitigation agreements were an unsatisfying way to address a

broader problem. CFIUS made it harder to compromise U.S. networks by buying a U.S. company. But foreign governments have other ways to compromise U.S. networks. They can provide subsidies so their own companies can underbid U.S. suppliers. If their price and quality are right, sooner or later the foreign companies will end up with a big share of the U.S. market—without ever making an investment that CFIUS can review. And if a company never makes a CFIUS filing, it will never have to sign a mitigation agreement, leaving some markets half-regulated.

Even more difficult to police is the supply chain. IT hardware and software are assembled from components made all over the world. A foreign government seeking to compromise U.S. computers doesn't need to buy Dell, or Intel, or Microsoft. It could buy a hard drive maker, a motherboard assembler, a modem supplier, even a keyboard manufacturer. Any of those components can be the source of computer security compromises. Again, without an investment in a U.S. company, CFIUS can do nothing about a "supply chain attack."

Even so, we had made a start, and a good one. Partial as they were, CFIUS mitigation agreements were still the best tool in our toolkit. They helped to close off the quickest and most obvious route that foreign governments might follow to compromise U.S. communications and data. Best of all, we seemed to have strong popular support for careful scrutiny of foreign acquisitions. If anything, the public had been convinced by the Congressional and media flap over DPW that CFIUS review was too lax.

In the end, though, DPW was poisoned fruit. The unjustified abuse that Congress had heaped on DPW eventually spurred a backlash. But when it came, it was aimed not at the worst Congressional offenders but at DHS.

Using CFIUS to reduce cybersecurity vulnerabilities was DHS's key strategy. As we turned mitigation agreements into a regulatory tool, we were drawing fire. And from some of the same forces that opposed us when we used new tools to deal with the risk of jet travel—business and the international community.

These forces slowly turned the DPW case into a millstone around the necks of the security community. At first, they concentrated on stopping the congressional effort to enact legislation that would make CFIUS tougher. Business groups quietly communicated their concern about the bill's effect on investment. After the initial burst of enthusiasm, work on the bill slowed. Nothing had been enacted by the midterm elections of 2006, in which Democrats took control of both the House and Senate. Although they had been loud in condemning the DPW deal while out of power, by the time they took control, those calls had muted.

Congress was now hearing from other governments as well as business. Other governments have no reason to encourage the United States to protect its national security through CFIUS. In fact, some governments have a direct interest in precisely the opposite. But even for our friends, there's no reason to praise CFIUS. The safest—and most conservative—stance was disapproval, and the DPW case certainly offered plenty of fodder for that position.

Many governments claimed to see a protectionist motive in CFIUS. For some, the accusation of protectionism was clearly a projection of their own inclinations. France, famously, had decided in 2005 that a French yogurt company was a "jewel" of French industry and therefore could not be sold to Pepsi. The Germans had refused to let foreigners buy into their auto industry. But the best defense is a good offense, the Europeans had learned; so European and other trade negotiators began to criticize U.S. CFIUS practice, hinting that it would have to be negotiated away in the next round of trade talks.

In the United States, unease about CFIUS spread to businesses that depended on foreign companies—from Wall Street investment banks to K Street lawyers. They too began quietly campaigning against the new regulatory push. They didn't want to see the United States opened further to espionage or sabotage, of course. But couldn't we do that without cutting off their deal flow?

The Alcatel-Lucent "evergreen" clause added to the tumult. From a foreign investor's point of view, the one good thing about CFIUS was

its certainty; once a deal cleared, it was cleared for good. It was a safe harbor against future storms. By adding an evergreen clause to the mitigation agreement, though, we had torn down the breakwater, leaving Alcatel and perhaps others exposed to future national security storms.

For foreign investors and their lawyers, the evergreen clause offered a second issue to rally round. In our view, the furor over the provision was out of all proportion to how often it was likely to be used. The fines and other enforcement measures that DHS had introduced were almost always tough enough to keep companies on the straight and narrow. Evergreen clauses were worthwhile only when normal incentives might not be enough to ensure compliance (usually when we feared that a foreign government could force the foreign company to take actions without regard for the company's own financial interests).

Part of the problem was perception. We couldn't talk about individual cases, and we didn't tell the parties to the transaction what our intelligence said about the buyer. So from the outside, our decisions did not look consistent or predictable. Sometimes we'd oppose a deal fiercely because intelligence revealed dangers that weren't obvious to outside observers, or even the parties. To outsiders, the role of intelligence in CFIUS was deeply frustrating, because it deprived them of the opportunity to rebut the charges.

They weren't wrong to be concerned. Intelligence is never perfect, and it should always be challenged before it is relied upon. Some of the CFIUS agencies didn't have a broad understanding of intelligence, and they sometimes gave it too much credence. (From time to time, I would propose audits or inspections of foreign buyers as a way of checking what the intelligence agencies were saying, but it was not easy to get the buyers to agree. Perhaps they didn't understand that an inspection might help them by providing a check on the intelligence—or perhaps they feared that it would confirm what the intelligence was telling us.)

The backlash against CFIUS was also aided from within. CFIUS has a peculiar structure that is almost guaranteed to spur bitter conflict. Originally established as a committee of cabinet members

headed by the treasury secretary, the committee has gradually added members from the White House bureaucracy. So, in addition to cabinet departments like Defense, State, DHS, Justice, and Commerce, the table is cluttered with representatives from the U.S. trade negotiating office, the Office of Science and Technology Policy, the National Security Council, the National Economic Council, and so on and so on. I say cluttered because these offices could talk but did not vote on transactions.

The White House offices are, in theory, at the table to protect the president. The idea is that their advice will be conveyed confidentially to the president if and when the committee makes a formal recommendation. That's the theory. In fact, the White House agencies all have turf struggles with each other, and they're often at the table to fight their rivals, or in the hope of influencing the debate before it reaches the White House.

White House staff didn't vote in CFIUS cases. But that hardly mattered, because votes were rarely useful. CFIUS is not an agency, and the Treasury Department, though it chairs the committee, is little more than first among equals. The purpose of the committee is to make a recommendation to the president. If one cabinet secretary wants to say something to the president, and another secretary is adamant that something else must be said, the treasury secretary will not be able to resolve the dispute. Both messages will be delivered.

And, given the institutional interests of the departments, it was almost inevitable that disagreements would arise. The State Department, for example, is always concerned about the reaction of foreign nations to our CFIUS decisions, and foreign nations never welcome a tough CFIUS regime. So State invariably opposed for as long as it could any effort to put conditions on transactions. The Office of the U.S. Trade Representative (USTR) was, if anything, even more predictable in opposing the use of CFIUS for cybersecurity purposes.

DHS, in contrast, was among the most likely to propose mitigation agreements or outright vetoes of risky deals. With Justice and the Defense Department, DHS formed the heart of CFIUS's national

security wing. Less predictable, at least over time, were Treasury and Commerce. Treasury is deeply sensitive to the mood of foreign investors, and that tended to push it toward the State Department. But it also had a large security role in stopping terrorist finance, and it was constrained by the need to act as chair of the committee, muting its natural sympathies. The Commerce Department speaks for U.S. business interests; some of its leaders thought that was enough to determine their position in CFIUS cases. Under other leadership, though, Commerce would sometimes give weight to its own national security arm, the office that oversees export controls on high technology and recognizes the risk posed by potential compromises.

There was a deep divide between the "national security" agencies and the "trade" or "economic" agencies. And, because Treasury could never force a decision over an impassioned dissent, arguments at CFIUS, particularly at the lowest levels, had a kind of well-worn vitriol to them. Everyone knew that the dispute would go higher. The only reason to pull back was fear that your boss wouldn't support you. At DHS, that was never a problem. We had short lines of communication and decisive leaders at the top. The secretary and deputy secretary could absorb new information and pass judgment on a course of action in minutes. Other agencies with less certainty of their boss's views were less willing to hold firm, and that sometimes helped us advance our cybersecurity agenda.

In the long run, though, the DPW flap hurt us badly. As the panic wore off, policymakers all across the government began to realize that they had been foolish to make such an issue of the DPW investment. That had been DHS's view all along. We thought the DPW case was a distraction from the greater dangers in telecom and information technology. For the business and international interests that opposed those measures, though, DPW was a godsend. Everyone knew that DPW had been a serious overreaction, and it was easy to lump everything together and argue that CFIUS was being abused.

As that idea took hold, CFIUS meetings grew more divided. Decision makers at the top of the Commerce Department or the U.S.

Trade Representative's office might not know much about cybersecurity, but they were happy to take a stand against CFIUS abuse. They began to back their lower-level officials more frequently on that basis. And so a logjam of unresolved conflict over CFIUS issues began to creep higher up the decision chain.

Deadlock became the norm. Trade agencies in particular would exercise a "bureaucrat's veto" by insisting that nothing could be done without their agreement and then asking for more paper, more process, and more debate before that agreement could be granted. They didn't say no, they just asked for more time.

Everyone in government is familiar with this tactic. The power to delay is often the power to prevent a policy decision. It was one more weapon in the arsenal of the institutional conservatives trying to prevent new policies from being adopted.

But delay had unexpected costs. The thirty-day deadline for decisions on most transactions was increasingly ignored. Too often, CFIUS would launch forty-five-day "investigations" simply to give the contending agencies more time to resolve their differences. Or it would strong-arm companies into "withdrawing" their applications and refilling them, starting the clock over again.

Much of this delay was caused by a growing determination on the part of the trade agencies to fight over the terms of mitigation agreements. But from the outside, all that the parties knew was that CFIUS was slowing their deal. For the trade agencies, this was a twofer. Their stalling tactics made it harder to get tough new mitigation agreements. And the delays brought the entire CFIUS process into disrepute, which increased the business backlash against strong CFIUS review.

Of course, the delay was hard on the companies involved in the transaction, but the trade agencies only occasionally seemed bothered by that. In fact, while DHS was viewed from the outside as the principal source of CFIUS scrutiny, and thus of delays, we were often the only voice arguing that the process should move more quickly to protect investors' need for certainty and promptness.

Officials who joined the administration after DPW also brought with them views shaped by the public debate but not informed by the intelligence that had driven our decisions in particular cases. Without access to that information, they tended to assume that all CFIUS decision making had been as irrational as the DPW case.

The National Security Council in particular suffered from this effect, and by 2007 it had abandoned any pretense of being an honest broker in CFIUS disputes. It became instead the principal combatant, working relentlessly to cut back the tough new security regime that we had introduced to CFIUS.

The critical showdown would come over who could negotiate and sign mitigation agreements. There was a long tradition of agency autonomy in this area. For years, mitigation agreements had been viewed as agreements with individual CFIUS members, not with CFIUS as a whole.

"This proposed mitigation agreement is between you and DHS," we used to tell companies when we tabled a draft. "It is meant to address the concerns that DHS has about your transaction. If we negotiate a satisfactory agreement, DHS will not oppose the transaction. We're not speaking for CFIUS, so there's always a possibility that the committee will disapprove the deal notwithstanding this agreement. And if we don't reach agreement, your deal may still be approved. You are simply taking the risk that DHS will oppose the deal and that we'll be able to persuade CFIUS not to approve it."

Because we were negotiating only for DHS (and sometimes for other agencies with similar concerns), it was easy for us to agree on tactics, priorities, and reach agreement on a deadline. That autonomy and flexibility is what allowed DHS to sign the quick mitigation agreement with DPW that was the administration's best defense during the Washington panic over the case.

For the trade agencies, though, that was all history. As far as they were concerned, DHS's authority to sign mitigation agreements had to be taken away. First, they argued that DHS and other agencies negotiating mitigation agreements should keep the rest of CFIUS

informed about the progress of the talks; then they argued that DHS should take their views into account in negotiating the agreements. Both of those positions sounded perfectly reasonable, but we accepted them with foreboding.

In theory, consultation with other agencies may provide useful new perspectives or avoid problems. In government practice, however, a consultation requirement is just a first step; it allows the consulted agency to second-guess and interfere, because it gives the agencies a chance to probe for weak spots. That is what happened in CFIUS. The trade agencies had little interest in helping the security agencies improve their mitigation agreements. Their principal interest was gaining enough information to argue that no mitigation agreement was necessary. Some of the more extreme agencies even violated the spirit and perhaps the letter of the CFIUS confidentiality requirements by "coaching" parties, suggesting arguments they should make when negotiating with DHS and then seconding those arguments in internal debates.

Eventually, the trade agencies began to insist that they weren't being consulted in good faith if DHS reserved the right to sign an agreement while the trade agencies were still asking questions. Consultation, in other words, couldn't end until the trade agencies agreed that all their questions had been answered. Of course, that formulation simply meant that the trade agencies could stall an agreement for as long as they could think up new questions. Or, more commonly, for as long as they could find new ways to ask the same old questions.

Impatient with this effort to undercut DHS's authority in a backdoor fashion, DHS simply continued to sign mitigation agreements. The parties usually were happy to do the deals, and the quicker the better. They had no interest in the ideological issues being raised by the trade agencies; they just wanted to move on. The trade agencies believed that the willingness of the parties to accept DHS's terms was irrelevant. They thought the parties were simply knuckling under because they needed to get their deals done quickly. They thought it was bad policy to use the leverage of CFIUS approval to extract

security agreements that would not apply to everyone in the industry. And they found DHS's refusal to be cowed more and more frustrating. Even at the deputy secretary level, conflict grew intense as CFIUS pressed DHS to give up its traditional authority to execute mitigation agreements.

By early 2007, the trade agencies and Treasury decided to take their frustration to Congress. The new Congress was led by Democrats, and they had made CFIUS reform a priority. But they were also listening to the business groups and foreign countries that had begun complaining about DHS's tough scrutiny. At a hearing to which DHS was not invited, its mitigation agreements were roundly criticized. Witnesses repeatedly bemoaned the fact that the number of mitigation agreements required by DHS tripled in 2006 from the previous three-year average (up from 4.5 to 15).

One witness expressed concern "that some agencies are taking undue advantage of the leverage inherent in CFIUS. CFIUS should not be a fishing expedition for a single agency to address comprehensive industry objectives on a "catch-as-catch-can" basis merely because they have leverage over one industry participant. … [I]f the Department of Homeland Security perceives a vulnerability in our telecommunications infrastructure, it should address that vulnerability across the sector, without regard to the ownership of firms."[5] Others made similar complaints.

Congress continued to insist that it wanted to make CFIUS tougher, but its actions said something else. Throughout the hearings and debates, congressmen touted the new bill as strengthening CFIUS and security. But when the television lights were turned off, the drafters sat down with the Treasury Department, and the committee leadership added language designed to undercut the authority of any agency to enter into a mitigation agreement on its own.

The new bill took the long overdue step of acknowledging the need for mitigation agreements, and it called for a "lead agency" in each case to negotiate the mitigation agreement. At the last moment, though, the House financial services committee leadership slipped in

an amendment to the bill, requiring that any mitigation agreement be negotiated "on behalf of the committee."[6] The effect of this modest phrase was dramatic. It would allow Treasury and the trade agencies to insist that they had to supervise the negotiation of any mitigation agreement now that the talks were being conducted "on behalf of" the entire committee. That meant that no negotiation could occur without a consensus among all CFIUS members. And that in turn meant that the trade agencies could use the "bureaucrat's veto" of endless delay to kill mitigation agreements even over the objection of the agency negotiating them.

The new CFIUS law[7] also contained a provision requiring that mitigation agreements be based upon a "risk-based analysis" of the threat to national security of the proposed transaction. The same manager's amendment described above also added language to this provision to specify that this analysis must be "conducted by the committee." This amendment gave the trade agencies a hand in analyzing national security threats and determining the level of appropriate mitigation. Once again, the committee leadership had reduced the security provided by CFIUS.

The House didn't exactly advertise the fact that it was weakening the hand of the security agencies. That wouldn't have been consistent with the dominant narrative in the press, where Congress was still loudly proclaiming the need to strengthen CFIUS because the administration hadn't given enough weight to security in the DPW case. Still, it seems likely that Congress knew exactly what it was doing. The business witnesses had asked that agency autonomy be abolished or constrained in the name of encouraging foreign investment, and as the Congressional Research Service noted, the amendment was adopted because the earlier bill, which lacked it, "could have delayed and discouraged foreign investment."[8]

International and business groups, in short, seem to have persuaded the committees that the real problem with CFIUS was not that it was too weak but that it was too tough. Needless to say, that wasn't a change of mind that Congress was eager to shout from the rooftops.

After the bill was enacted, the National Security Council wasted little time turning the "on behalf of" language into precisely what DHS had feared—a radical restriction in the authority of the security agencies. In fact, it built an entire edifice of obstruction on those few words. Under the executive order[9], the lead agency must achieve consensus within CFIUS before it can even propose a mitigation agreement. To do this, the agency must prepare a written statement that (1) identifies the national security risk posed by the transaction, including potential threats, vulnerabilities, and consequences, and (2) sets forth the mitigation measures, which must be "reasonably necessary" to address the risk.

After jumping through these hoops just to propose a mitigation measure, the lead agency must also get committee approval before negotiations can begin. It must keep the committee fully informed of its activities and must notify the Secretary of the Treasury in advance of any proposed major action, allowing time for the committee to consult and direct the lead agency about how it should act.

By the time the order was fully written, the lead agency was less a leader than an indentured servant. It might sit in the driver's seat, but every member of CFIUS would have a hand on the steering wheel and a foot on the brakes of the negotiations. The trade agencies were happy to use the brakes. No negotiations could occur, they would insist, until a final position had been agreed to by all agencies. This made the old tactic of delay and refusal to agree a potent weapon again. Security agencies were ordered not to even tell the parties to the transaction what their concerns were until they had the consent of the other agencies.

This quickly led to absurd results. In one case, when DHS expressed concerns about what might happen after the merger, the parties promised to take action after the merger that would completely resolve the worry. DHS suggested to the committee that the promise be put in writing so that the assurance was binding. Some members objected and the assurance was never formalized.

In another case, the deadlock in the committee went on so long that the parties wrote letters to all members of the committee begging

to be told what DHS wanted, arguing that it would much rather agree to reasonable mitigation conditions than wait for the committee to finish its internecine bureaucratic war. Nothing doing. The trade agencies were determined to make the United States safe for foreign investment no matter how many foreign investors they had to hurt in the process.

The most ironic note was sounded toward the end of the administration, when another foreign purchase of port facilities was submitted for approval. DHS proposed a modest mitigation agreement, similar to the DPW agreement that so many in Congress had condemned as inadequate during the panic. This time, though, under the law that Congress had enacted in reaction to DPW, even this modest agreement could not be imposed. The trade agencies refused to accept it, and Congress had made their consent a necessary condition to any mitigation agreement.

The counterattack on behalf of business and the international community had come a long way against heavy odds. The new law had been so trimmed and twisted that in the end the one part of the DPW affair that could not be repeated was the one part that contributed to security—the mitigation agreement.

The effect was felt quickly. In 2008, the number of mitigation agreements fell dramatically, and they became even more rare in 2009.

In the end, though, much of what DHS did to make CFIUS a force for network security endured. Even in the waning days of the administration, long after the new CFIUS law and executive order took effect, a new transaction raising severe security concerns came to CFIUS. Working with the other security agencies, DHS made the case against the deal. Faced with evidence of grave risk, the trade agencies folded; they did not oppose our recommendation that the transaction be rejected. Had the security agencies been willing to execute a mitigation agreement, they would have accepted that recommendation as well.

The lesson of that transaction was that the trade agencies would not fight the security agencies when the chips were down. Security is

the mission of DHS, Defense, and Justice. If those agencies say with confidence that a transaction will raise serious security concerns, it is hard for an agency like USTR to second-guess them. And at the highest levels, each agency tends to take a broader view than simply its own bureaucratic interest. This means that, for transactions that raise the greatest concern, the new law is not fatal to the reforms that DHS pioneered.

Still, the story shows how hard it is to regulate even the most dangerous cybersecurity threats. CFIUS dealt with the particularly overt and troubling threats, and in most cases it had found a way to allow investments to go forward, though with safeguards.

Even so, the nations and companies that opposed any regulation had successfully advocated for a law and executive order that undermined the security agencies, at least somewhat. That they accomplished their mission in the teeth of noisy public demands for tougher CFIUS security standards is a testament to their formidable clout.

The Hoover Institution on War, Revolution and Peace, founded at Stanford University in 1919 by Herbert Hoover, who went on to become the thirty-first president of the United States, is an interdisciplinary research center for advanced study on domestic and international affairs. The views expressed in its publications are entirely those of the authors and do not necessarily reflect the views of the staff, officers, or Board of Overseers of the Hoover Institution.

www.hoover.org

Hoover Institution Press Publication No. 591

Hoover Institution at Leland Stanford Junior University,
Stanford, California, 94305–6010

First printing 2010
16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1

Manufactured in the United States of America

The paper used in this publication meets the minimum Requirements of the American National Standard for Information Sciences—Permanence of Paper for Printed Library Materials, ANSI/NISO Z39.48-1992. ♾

Cataloging-in-Publication Data is available from the Library of Congress.
ISBN-13: 978-0-8179-1154-6 (cloth)

ISBN-13: 978-0-8179-1156-0 (e-book)