
3

THE BRITTLE SUPERPOWER

Stephen E. Flynn

The United States has been living on borrowed time – and squandering it. In the four years since the September 11, 2001, attacks on the World Trade Center towers and the Pentagon, the Bush administration has chosen to emphasize the use of military operations overseas over an effort to reduce America’s vulnerability to catastrophic terrorist attacks at home. While the administration has acknowledged in principle the need to improve critical infrastructure protection, in practice it has placed the burden for doing so primarily on the private sector that owns and operates much of that infrastructure. But this delegation of responsibility fails to acknowledge the practical limits of the marketplace to agree upon common protocols and to make investments to bolster security. As a result, the transportation, energy, information, financial, chemical, food, and logistical networks that underpin U.S. economic power and the American way of life remain virtually unprotected. The tragic loss of life in the aftermath of Hurricane Katrina in 2005 exposed Washington’s shocking lack of preparedness to respond to large-scale disasters on American soil. The United States may be the world’s sole superpower, but it is showing ominous signs of being a brittle one. If the federal government does not provide meaningful incentives to make U.S. infrastructure more resilient and create workable frameworks for ongoing public and private partnerships to advance security, future terrorist attacks and natural disasters with profound economic and societal disruption are inevitable.

It does not have to be this way. Given the wealth of the United States, it can clearly afford to invest in measures that will make America a more resilient society in the face of human-caused and natural disasters. But critical

This chapter is adapted from Flynn 2004. The author retains the copyright for this chapter.

infrastructure protection and emergency preparedness will not happen if left solely to the marketplace. Nor can they be accomplished solely at the local and state levels. Instead, the federal government should be taking the lead in engaging the private sector in a collective effort to confront the threat of catastrophic acts of terror and natural disasters at home. Unfortunately, while the post-9/11 case for homeland security is seemingly a straightforward one, Washington has demonstrated an extraordinary degree of ambivalence about making any serious effort to tackle this mission. Instead, the White House has favored muscular efforts abroad to combat terrorism and has passed along the emergency preparedness mission to governors, county commissioners, and mayors. The premise behind the Bush administration's strategy of preemptive use of force is that as long as the United States is willing to show sufficient grit, it can successfully hold its enemies at bay. Throughout the 2004 presidential campaign, the President and Vice President asserted that the war on terror had to be waged at its source. In the words of Vice President Dick Cheney, "Wars are not won on the defensive. To fully and finally remove this danger [of terrorism], we have only one option – and that's to take the fight to the enemy."¹ On July 4, 2004, President Bush made the point this way: "We will engage these enemies in these countries [Iraq and Afghanistan] and around the world so we do not have to face them here at home."²

Targeting terrorism at its source is an appealing notion. Unfortunately, the enemy is not cooperating. As the March 2004 attacks in Madrid, July 2005 attacks in London, August 2005 attacks in Sharm el Sheikh, Egypt, and October 2005 attacks in Bali, Indonesia, have made clear, there is no central front on which Al Qaeda and its radical jihadist imitators can be cornered and destroyed. Terrorist organizations are living and operating within jurisdictions of U.S. allies and do not need to receive aid and comfort from rogue states. According to the U.S. Department of State's annual global terrorism report, the number of terrorist incidents was at a record high in 2004, despite the U.S.-led invasions of Afghanistan and Iraq.³ There is mounting evidence that the invasion of Iraq is fueling both the number of recruits and the capabilities of radical jihadist groups.⁴

The reluctance of the White House and the national security community to adapt to the shifting nature of the terrorist threat bears a disturbing resemblance to the opening chapter of World War II. In September 1939, the German army rolled eastward into Poland and unleashed a new form of combat known as "blitzkrieg." When Poland became a victim of the Third Reich, London and Paris finally abandoned their policies of appeasement and declared war. The British and French high commands then began to execute war plans that relied on assumptions drawn from their experiences in World War I. They activated

their reserves and reinforced the Maginot Line – defenses of mounted cannons stretching for 250 miles along the Franco–German border. Then they waited for Hitler’s next move.

The eight-month period before the fall of Paris came to be known as “the phony war.” During this relatively quiet time, France and the United Kingdom were convinced they were deterring the Germans by mobilizing their more plentiful military assets in an updated version of trench warfare. But they did not alter their tactics to respond to the new offensive warfare that the Germans had executed with such lethal results in eastern Europe. In May 1940, France and the United Kingdom paid a heavy price for their complacency: Panzer units raced into the lowlands, circumvented the Maginot Line, and conquered France shortly thereafter. The British expeditionary forces narrowly escaped by fleeing across the English Channel aboard a makeshift armada, leaving much of their armament behind on the beaches of Dunkirk.

Instead of a Maginot Line, the Pentagon is executing its long-standing forward defense strategy, which involves leapfrogging ahead of U.S. borders and waging combat on the turfs of U.S. enemies and allies. Meanwhile, protection of the rear – the American nation itself – remains largely outside the scope of national security, even though the 9/11 attacks were launched from within the United States against targets on American soil.

Al Qaeda has demonstrated that by directing terrorist attacks on major urban areas and the critical foundations of modern life, it can generate a very “big bang for their buck.” Al Qaeda also placed the United States at the top of its target list and made clear that it wants to carry out a more devastating attack than those on New York and Washington.⁵

Defenders of the Bush administration’s war on terrorism are quick to point to the absence of another 9/11-style attack on U.S. soil as vindication for placing overwhelming emphasis on an offense-oriented strategy. To be sure, there is ample evidence that the war in Iraq has been attracting foreign insurgents and Al Qaeda sympathizers to Baghdad versus to Main Street. However, this is likely to prove to be a short-term reprieve that poses a longer-term danger. Beginning in June 2003, Iraq’s energy sector became a primary target for insurgents. By mid-July 2005, nearly 250 attacks on oil and gas pipelines had cost Iraq more than \$10 billion in lost oil revenue. Successful attacks on the electrical grid have kept average daily output at 5 to 10 percent below the pre-war level, despite the \$1.2 billion the United States has spent to improve Iraqi electrical production.⁶

In some ways, the situation in Iraq is analogous to what happened during the decade-long conflict from 1970 to 1989 against the Soviet occupation of Afghanistan. The foreign participants who joined the mujahideen in that conflict became the hardened foot-soldiers who would ultimately transform themselves into Al Qaeda. But unlike Afghanistan, where the combatants

waged war in a pre-modern society, insurgents in Iraq are refining their skills to sabotage critical infrastructures. Accordingly, when these foreign insurgents eventually return to their native lands, they will do so with the experience of successfully targeting complex systems that support economic and daily life within advanced societies.

Even if the United States had not chosen to invade Iraq, an alternative scenario explains why there has not been another attack on American soil. As a practical matter, sophisticated terrorist operations on the scale of the 9/11 attacks take time. Because Al Qaeda has proclaimed that it wants to surpass the destruction and disruption associated with toppling the World Trade Center towers, the current period of quiet may indicate a lull during which the organization is focusing on meticulously planning its next large-scale operation. Deploying the complex organizational structure to carry out those plans could take several years. This is because such an attack typically involves deploying a three-cell structure in which the members of each cell are isolated from one another to ensure the greatest chance of survival if any one cell is compromised.

An Al Qaeda-style operation involves a “logistics” cell to attend to such things as locating safe houses, providing identity documents, and finding jobs for the operatives so they can blend into the civilian population. In addition, a “surveillance” cell is charged with scoping out potential targets, probing security measures, and conducting dry runs. Finally, an “attack” cell may include suicide bombers who are charged with executing the attack.⁷

Establishing extensive organizational capacity is a painstaking process, particularly within the United States, where Al Qaeda must work from a much smaller footprint of operatives and sympathizers than it has in Western Europe or countries like Indonesia. Terrorist cells are also a resource that must be carefully husbanded, because using them will likely translate into losing them. This is because it is impossible to carry out an attack without leaving some forensic clues that expose the cells to enforcement action. Accordingly, cells that go after what would seem to be a plentiful menu of soft targets such as shopping malls or sporting events can generate plenty of short-term media attention. But if these attacks cannot be sustained over time (because the authorities are able to track down and destroy the terrorists’ organization), the long-term economic consequences are likely to be modest. As a result, terrorists will want to make sure that they pick meaningful targets where the attack proves to be worth all the organizational effort to carry it out.

In short, it would be foolhardy to act as though the 9/11 attacks were an aberrant event in which Al Qaeda got lucky because America’s guard was temporarily down. The sad truth is that America’s guard was never really up, and despite all the political rhetoric, little has changed in recent years. The most tempting targets for terrorists remain those that can produce widespread economic and

social disruption. However, the White House has declared that safeguarding the nation's critical infrastructure is not really a federal responsibility. According to President Bush's 2002 National Homeland Security Strategy, "The government should only address those activities that the market does not adequately provide – for example, national defense or border security. . . . For other aspects of homeland security, sufficient incentives exist in the private market to supply protection."⁸ This expression of faith, however, has not borne out. According to a survey commissioned by the Washington-based Council on Competitiveness just one year after the 9/11 attacks, 92 percent of executives did not believe that terrorists would target their companies, and only 53 percent of the respondents indicated that their companies had increased security spending between 2001 and 2002.⁹ With the passing of each month without a new attack, the reluctance of companies to invest in security has only grown.

The lack of enthusiasm among company executives to provide leadership when it comes to developing the means to safeguard critical infrastructures should not be surprising. This is because survival in the marketplace has required that they be responsive to four globalization imperatives for making critical infrastructures (1) as open to as many users as possible; (2) as efficient as possible; (3) as reliable as possible; and (4) as low cost as possible to use. Because the conventional view of security is that it raises costs, undermines efficiency, is at odds with assuring reliability, and constrains access, there has been a clear disincentive for the private sector to make it a priority. As a result, the United States entered the twenty-first century with networks that have an extraordinary capacity to generate wealth but with few meaningful safeguards in the event of an attack.

The challenge of elevating the critical infrastructure protection priority and crafting a tidy security division of labor between the private and public sectors is complicated by two additional factors. First, safeguards that only apply within U.S. borders will not work because the United States' critical infrastructures depend on their links to the rest of North America and the world. Second, the United States competes in a global marketplace, and it must be mindful of not unilaterally incurring costs that place U.S. companies and the U.S. economy at a competitive disadvantage.

Private sector concerns about maintaining competitiveness in the face of the growing security imperative are legitimate. Security is not free. A company incurs costs when it invests in measures to protect the portion of infrastructure it controls. If a company does not believe other companies are willing or able to make a similar investment, then it faces the likelihood of losing market share while simply shifting the infrastructure's vulnerability elsewhere. If terrorists strike, the company still suffers the disruptive consequences of an attack right alongside those who did nothing to prevent it. Those consequences are likely

to include the cost of implementing new government requirements. Therefore, infrastructure security suffers from a dilemma commonly referred to as the “tragedy of the commons.”

Take the case of the chemical industry. By and large, chemical manufacturers have a good safety record. But security is another matter. Operating on thin profit margins and faced with growing overseas competition, most companies have been reluctant to incur the additional costs associated with improving their security. One plausible scenario is that the manager of a chemical plant will look around his facility and gets squeamish about the many security lapses he finds. After a fitful night’s sleep, he will wake up and decides to invest in protective measures that raise the cost to his customers by \$50 per shipment. A competitor who does not make that investment will be able to attract business away from the security-conscious plant because his handling costs will be lower. Capable terrorists and criminals will then target this lower-cost operation because it is an easier target. In the event of an attack, particularly one that is catastrophic, two consequences are likely. First, government officials will not discriminate between the more security-conscious and the less security-conscious companies. All chemical plants are likely to be shut down while the authorities try to sort things out. Second, once the dust clears, elected and regulatory officials will scramble to impose new security requirements that could nullify the proactive plant owner’s earlier investments. Given this scenario, the most rational behavior of the nervous manager would appear to be to keep tossing and turning at night while focusing on short-term profitability during the day.

The only way to prevent the tragedy of the commons is to convince all the private participants to abide by the same security requirements. When standards are universal, their cost is borne equally across a sector. As taxpayers or as consumers, Americans will end up bankrolling these measures, but what they will be paying for is insurance against the loss of innocent lives and a profound disruption to their society and the economy.

The problem boils down to this: the design, ownership, and day-to-day operational knowledge of critical systems rest almost exclusively with the private sector. But security and safety are public goods whose provision is a core responsibility of government at all levels. The government is unable to protect things that it has only a peripheral understanding and limited jurisdictional reach, and the market will resist providing public goods if doing so puts them at a competitive disadvantage by eroding their profits or sacrificing their market share.

Certainly, the 9/11 attacks created a general sense among public and private sector players that the security imperative requires far more attention than it had been receiving. But the reality is that there still remain disincentives

for the private sector to cooperate with government entities on this agenda. Some of the structures in place, such as the laws and regulations that guide the interaction within and among these sectors, remain static. For instance, anti-trust laws severely constrain the ability of industry leaders to come together and agree to common protocols. Also, companies that make a good faith effort to undertake industry-generated anti-terrorist measures potentially risk open-ended liability issues should terrorists succeed in defeating those measures. After the post-mortem, public officials are likely to be the first at the head of the queue insisting that private sector entities be held accountable for not having done enough.

While there are practical barriers to having the private sector assume the bulk of the responsibility for the post-9/11 security mandate, leaving it to the public sector alone to map the path ahead holds little promise as an alternative. When the government announces requirements or “best practices” after a lengthy deliberative process with nominal industry input, it almost always misses the mark. More often than not, the proposed or mandated safeguards reflect a poor understanding of the design and operation of critical infrastructures and the real versus perceived vulnerabilities. This disconnect is because many of the most critical issues span multiple agency jurisdictions, and these agencies rarely work well together. The results end up being a mix of unacknowledged gaps and redundant requirements.

If improving homeland security requires that the U.S. government reconsider many of its assumptions and priorities, it also requires a population that acknowledges that security must become everyone’s business. The starting point for engaging civil society in this enterprise is a willingness to accept that there will never be a permanent victory in a war on terrorism by overseas military campaigns. Terrorism is simply too cheap, too available, and too tempting to ever be totally eradicated. And U.S. borders will never serve as a last line of defense against a determined terrorist. What is required is that everyday citizens develop both the maturity to live with the risk of future attacks and the willingness to invest in reasonable measures to mitigate that risk.

This is not a defeatist position. Improving the United States’ protections and its resilience to withstand acts of catastrophic terrorism has both tactical value in preventing these attacks and strategic value in deterring them in the first place. Radical jihadist groups do not have unlimited resources. When they strike, they want to be reasonably confident that they will be successful. They also want to inflict real damage that will generate political pressure to adopt draconian measures in response to a traumatized public.

Today’s terrorist masterminds know that the main benefit of attacks on critical infrastructure is not the immediate damage they inflict, but the collateral consequences of eroding the public’s trust in services on which it depends.

Certainly this lesson has not been lost on Osama bin Laden. In a video tape broadcast on *Aljazeera* on November 1, 2004, bin Laden claims: “for example, Al Qaeda spent \$500,000 on the event, while America, in the incident and its aftermath, lost – according to the lowest estimate – more than \$500 billion. Meaning that every dollar of Al Qaeda defeated a million dollars by the permission of Allah, besides the loss of a huge number of jobs.”¹⁰

What if the next terrorist strike were on the American food supply system? The attack itself might kill only a handful of people, but without measures in place to reassure the public that follow-on attacks could be prevented or at least contained, consumers at home and abroad would become distrustful of a sector that accounts for more than 10 percent of U.S. gross domestic product. Similarly, a dirty bomb smuggled in a container and set off in a seaport would likely kill only a few unfortunate longshoremen and contaminate several acres of valuable waterfront property. But if there is no credible security system to restore the public’s confidence that other containers are safe, mayors and governors throughout the country, as well as the President, will come under withering political pressure to order the shutdown of the intermodal transportation system. Examining cargo in tens of thousands of trucks, trains, and ships to ensure it poses no threat would have devastating economic consequences. When containers stop moving, assembly plants go idle, retail shelves go bare, and workers end up in unemployment lines. A three-week shutdown could spawn a global recession.

As long as catastrophic terrorism is assured of generating a huge bang for the buck, current and future U.S. adversaries will make it the first arrow they reach for in attacking the country. Their confidence in their ability to inflict real damage on the world’s sole superpower will be directly proportional to the unwillingness of private and public leaders to acknowledge the risk of market failures associated with excessive reliance on unprotected networks that are sophisticated, concentrated, and interdependent. Given the futility of terrorists taking on U.S. military forces directly, attacking these networks is not irrational. In warfare, combatants always seek to exploit their adversary’s weaknesses.

However, if terrorist attacks were likely to be detected, intercepted, contained, and managed without doing any measurable damage to the American way of life or quality of life, their value as a means of warfare would be depreciated. Because such acts violate widely accepted norms, they will almost certainly invite not just American, but also international, retribution. Most adversaries would probably judge this too high a price to pay if striking civilian targets holds out little chance of causing the desired mass disruption.

A focus on critical infrastructure protection can also improve the effectiveness of more conventional counterterrorism measures. By bolstering the

security of critical networks in advance of possible attacks, adversaries must put together more complex operations to target them successfully. The resultant need for terrorists to raise more money, recruit expertise, and lengthen planning cycles and rehearsals would be a boon for intelligence services and law enforcement officials. This is because such pre-execution activities elevate the opportunities for infiltration and raise the odds that terrorist groups will attract attention.

There is an added bit of good news that comes from placing greater emphasis on homeland security. The most effective measures for protecting potential targets or making them more resilient in the face of successful attacks almost always have derivative benefits for other public and private goods. For instance, bolstering the tools to detect and intercept terrorists will enhance the means available to authorities for combating criminal acts such as narcotics trafficking, migrant smuggling, cargo theft, and violations of export controls. The risk of an avian flu pandemic and outbreaks such as SARS, AIDS, West Nile virus, foot-and-mouth disease, and mad cow disease have highlighted the challenges of managing deadly pathogens in a shrinking world. Public health investments to deal with biological agents or attacks on food and water supplies will provide U.S. authorities with more effective tools to manage these global threats. Measures adopted to protect infrastructure make it more resilient not only to terrorist attacks, but also to “acts of God” or human and mechanical error. They also invariably reinforce U.S. values that are respected around the world, whereas reliance on aggressive military measures invariably puts those values at risk.

How much security is enough? Answering that question requires identifying both the threat a security measure is designed to counter and the appropriate point at which an additional investment in a security measure yields only a marginal return. Asking members of the private sector to decide independently where this line should be drawn is impractical because they lack access to intelligence and because they need good-Samaritan safeguards should their efforts fall short of deterring every terrorist incident. Only the federal government has access to threat information, and only the federal government can establish liability limits.

In the end, the threshold for success will be met when the American people can conclude that a future attack on U.S. soil will be an exceptional event that does not require wholesale changes in how they go about their lives. This means that they should be confident that there are adequate private and public measures in place to confront the danger and manage its aftermath. In other words, homeland security should strive to achieve what the aviation industry has done with safety. It has been the aviation industry’s long-standing and ongoing investments that have sustained air travel (despite the periodic horror of airplanes falling out of the sky) and have convinced the public that it is safe

to fly. Public confidence can never be taken for granted after a major jet crash, but private and public aviation officials start from a credible foundation built upon a cooperative effort to incorporate safety into every part of the industry. In the immediate aftermath of airline disasters, the public is reassured by the fact that the lessons learned are quickly compiled and released and that the government and the industry seem willing to take whatever corrective actions are required.

Ongoing and credible efforts to confront risk are essential to the viability of any complex modern enterprise. Aviation safety provides helpful reference points for how to pursue security without turning the United States into a national gated community. First, it demonstrates that Americans do not expect their lives to be risk-free; they just rightfully expect that reasonable measures be in place to manage that risk. Second, managing risk works best if safeguards are integrated as an organic part of a sector's environment and if they are dynamic in adapting to changes in that environment. Third, government plays an essential role in providing incentives and disincentives for people and industry to meet minimum standards. Security simply will not happen by itself.

When it comes to critical infrastructure protection, the issue, then, is to engage the private sector to develop standards and create effective mechanisms for their uniform enforcement. This is a task that necessitates a much different kind of institutional framework than setting up a new federal department of homeland security. What it requires is the creation of a structure that allows the private sector and civil society to participate as equal partners in the process of designing and implementing security for the U.S. homeland.

Admittedly, it will not be easy to muster the political will to admit the post-9/11 error of placing so much emphasis on projecting military might abroad while neglecting efforts to build greater U.S. resilience at home. But now is not a time for timidity. Americans and private sector leaders must demand that Washington make homeland security generally and critical infrastructure specifically a priority. And the entire nation, not just the national security establishment, must be organized for the long struggle against terrorism.

NOTES

1. Remarks by the Vice President at the 123rd Coast Guard Academy Commencement (White House 2004b).
2. White House 2004a.
3. U.S. Department of State 2005. The report does not include the specific figures but states in its overview: "Despite ongoing improvements in U.S. homeland security, military campaigns against insurgents and terrorists in Iraq and Afghanistan, and deepening counterterrorism cooperation among the nations of the world, international terrorism

continued to pose a significant threat to the United States and its partners in 2004.” However, the *Washington Post* reports that congressional aides briefed on the U.S. Department of State statistics confirmed that the number of serious terrorist incidents tripled in 2004 (Glasser 2005).

4. Clarke 2004.
5. CNN 2002.
6. See Benjamin and Simon 2005.
7. Flynn 2005c.
8. White House 2005b.
9. Council on Competitiveness 2002.
10. Aljazeera 2004.