The US Army War College Quarterly: Parameters

Volume 38
Number 4 *Parameters Winter 2008*

Article 3

11-1-2008

Preserving Infrastructure: A 21st Century Challenge

Michawel Certoff

Recommended Citation
Michawel Certoff, "Preserving Infrastructure: A 21st Century Challenge," *Parameters* 38, no. 4 (2008), doi:10.55540/0031-1723.2446.

Preserving Infrastructure: A 21st Century Challenge

MICHAEL CHERTOFF

As the United States marked the seventh anniversary of the 9/11 attacks and the fifth anniversary of the creation of the Department of Homeland Security (DHS), one of the most urgent tasks remained the continued protection of the nation's critical infrastructure. Since its principal function is to protect the nation, government has a vital role to play. But what kind of role should this entail?

Broadly speaking, there are two possible answers to this question. The first possibility is what might be deemed the government-alone answer. This approach calls for businesses that operate infrastructure to be intensively managed by officials in Washington, D.C., or state capitals. Those who endorse this view hold that the best way to reduce vulnerabilities is by placing government hands on all the control levers. They also believe that an optimal strategy for countering threats is to put "boots on the ground" in order to guard facilities.

With heavy concentrations of uniformed guards and detailed mandates being imposed from the top down, this approach hearkens back to the classic command-and-control model from the previous century. A number of people in Washington would like government to apply this philosophy to homeland security challenges. When it comes to cargo security, for example, they want Customs and Border Protection officers overseas to physically inspect every shipping container before it is sent to America. If we refrain from doing so, they argue, we are being dangerously lax in guarding against impending threats.

DHS has largely rejected this approach for a number of reasons. First, it is often based on the chimerical strategy of risk elimination. Eliminating every risk to the country's infrastructure is figuratively impossible. If implemented, the kinds of security measures required to pursue such a strategy could destroy what we are trying to protect, namely the normal, daily commerce of

the United States. If our officers physically inspected every piece of inbound cargo, it could grind commerce to a halt, effectively handing the terrorists the victory they desire. A second reason to avoid such a strategy is the fact that the federal government does not have the financial resources to shoulder 100 percent of America's homeland security responsibilities. It is beyond Washington's means to assume the burden of micromanaging every critical business activity in the United States or supplying sufficient personnel to guarantee a reduction in the vulnerabilities of these activities. Third, DHS rejected this strategy because those who own and operate businesses have a natural incentive to protect them. These owners and operators are normally cognizant of the risks they face, including security threats. They do not need to be told that if a flood or cyber attack destroys their computer system, they might be out of business.

Consequently, rather than pursuing the government-only approach, DHS favors an alternative strategy that treats the business community as an equal partner in strengthening its security. We want to hold businesses accountable, but not micromanage them. This partnership model allows businesses to engage in the familiar task of risk management—creating security measures and channeling resources where the need is greatest—rather than being compelled to pursue the quixotic goal of risk elimination. Such a strategy seeks to have businesses share in the burden of security enhancement. Instead of requiring commercial enterprises to provide a greater degree of protection for assets they already value, this approach affords them the ability to design and implement systems that reduce vulnerabilities, while simultaneously providing the security information and guidance required, as well as the standards and metrics allowing evaluation of progress. The objective is to leverage private-sector capabilities and incentives with federal know-how in an effort to achieve maximum risk reduction based on the most efficient use of resources.

Michael Chertoff was sworn in as the second Secretary of the US Department of Homeland Security on 15 February 2005.

The initiative identified those elements of critical infrastructure overseas that are closely intertwined with domestic industries.

Applying the Partnership

Three prominent examples provide a glimpse of how this twenty-first century partnership can be successful. The first involves a set of chemical security regulations that Congress authorized the Department of Homeland Security to issue. They were issued in response to an obvious vulnerability at certain chemical facilities located in high-population areas, facilities that terrorists might exploit, resulting in the catastrophic release of chemical agents.

In addressing this problem, the Department realized that the government-only solution was totally unrealistic. Placing guards at every chemical plant on a 24-hour basis while saddling the industry with a one-size-fits-all mandate would be prohibitively expensive to the government and the chemical firms. Such a strategy actually risked irreparable damage to the very industry DHS was attempting to protect. As an alternative to this strategy, DHS chose the partnership model. Working with Congress, industry, stakeholders, and academics, the Department developed a framework that focused on high-risk facilities, those with the most dangerous chemicals and surrounded by vulnerable population centers. The Department then established a hierarchy of risk. The facilities at greatest risk were in the top tier, while those facing lesser threats were ranked based on an analysis of their vulnerabilities and communities. Based upon the degree of risk, DHS directed companies to achieve specific performance measures. They were required to complete and submit security vulnerability assessments if they were in the high-risk category, develop site security plans, and implement risk-based measures that supported the performance standards.

Essentially, the Department was setting benchmarks that specified outcomes while permitting businesses to determine the most cost-effective strategies needed to fulfill them. It was a partnership, utilizing accountability, not bureaucracy.

Those who might believe this approach was all carrot and no stick would be incorrect. Companies had the right to decide how to reach the security goals outlined; those falling short were subject to penalties that included fines of up to $25,000 a day. This partnership model resulted in a realistic and workable security solution for the chemical industry. It established clear, achievable security requirements while permitting the responsible companies to find the best way to meet the goals outlined and penalized only those companies that failed to take appropriate action.

A second example of the partnership model may be found in the SAFETY Act, the Support Anti-terrorism by Fostering Effective Technologies Act of 2002. With Congress's help, DHS formalized liability protections that encouraged the technology industry to develop cutting-edge security solutions while limiting exposure to unnecessary and counterproductive litigation.

The third, and perhaps the most comprehensive, application of the model involved the implementation of the National Infrastructure Protection Plan. In unprecedented fashion, DHS brought together federal, state, and local governments in a partnership with the private sector to identify the nation's most critical infrastructure. Rather than establishing one master plan, this model is actually a collection of plans; 18 of them, each headed by a council, and each tailored to the needs and conditions of a specific sector of the economy. By means of interaction with the sector councils, DHS gets the best security ideas from the private sector while providing relevant information and intelligence. The goal is to achieve maximum advantage in protecting each of these sectors.

In developing this plan, the Department created a comprehensive list of nearly 3,000 national assets, systems, and networks across the 18 sectors. As a result, when there is a hurricane in the Gulf of Mexico or a series of wildfires on the West Coast, responding agencies know exactly what has to be protected or restored. The agencies also know what alternative mechanisms have to be used while a particular piece of infrastructure is out of commission. This visibility and the ability to go directly to economic and business actors have reduced the impact of disasters that otherwise might cascade across the country, impacting the nation's health, safety, security, and economic well-being.

International and Domestic Initiatives

DHS is conducting a focused survey of infrastructure and vulnerabilities not just at home but also abroad through the Critical Foreign Dependencies

Initiative launched in 2007. The initiative identified those elements of critical infrastructure overseas that are closely intertwined with domestic industries. We now know, for example, the effect on America's energy environment if a refinery shuts down somewhere in the world, or if closure of a natural gas field overseas might impact America's interests or status.

By identifying and focusing on overseas assets and systems upon which Americans are dependent, the government achieves two objectives. First, it can plan for the possibility of disruption. Second, it can help foreign partners and companies protect infrastructure. In short, the partnership approach remains a sound and sensible means of securing the lion's share of US and international infrastructure.

Yet there are unavoidable instances in which government has a much broader and deeper responsibility. The first such instance concerns "common goods," meaning infrastructure that is publicly owned and managed, serving wider interests beyond a particular manufacturer or business. This category includes bridges, highways, and levees—infrastructure which protects entire communities and is owned and operated by some level of government, whether local, state, or federal. In these cases, the government is required to assume full responsibility for ensuring adequate protection of designated infrastructure.

A second area involves infrastructure that is controlled by the private sector but is critical to other businesses and a major segment of the population. For example, companies focused on energy transmission are obligated not only to ensure that they are protecting their assets and employees, but to recognize that failure to do so will have a cascading effect on other businesses and people. When it comes to securing this privately owned but publicly indispensable infrastructure, government needs to play a greater role. Because the consequences of failure are so dire and the cascading effects so potentially diverse, an expanded role for government is imperative.

These strategies continue to serve the United States well in protecting its infrastructure from terrorism. Regrettably, the nation has not been as successful in protecting these vital assets against simple wear and tear and Mother Nature. Time and again, the appropriate agencies have failed to make the necessary long-term investments required to maintain critical structures against the physical ravages of time or protect them against natural disasters endemic to specific geographic areas.

Simply stated, the United States has not invested enough in the long-term maintenance of its levees, dams, and power grids. As a result of this

neglect, the nation spends an inordinate amount of money repairing this infrastructure when it fails. Once failure occurs, exponentially larger sums are required for response, relief, recovery, and rebuilding, all caused by an emergency that did not need to happen, had government pursued a disciplined plan of regular infrastructure investment.

Three prominent examples of governmental failure come to mind. The first is associated with the levee system in Sacramento, California, one of the top at-risk urban areas of the country for flooding. This area of California has experienced five record floods over the past half century. A catastrophic failure of levees in Sacramento would have a disastrous impact on the city's population and could potentially affect the watershed for much of California. Imagine the consequences of such a failure; a considerable part of America's most populous state would be without water for drinking and agriculture.

Yet for decades, what has stood between California and this apocalyptic scenario is a patchwork system of aging levees built more than a hundred years ago when the area was sparsely populated farmland. When the system was first constructed, if the levees were breached, the worst that could happen would be a flooded field. Today, with the area teeming with homes, people, and businesses, a great deal more is at risk. Sacramento is faced with a situation where the heightened risk of flooding, inadequate levee maintenance, and rapid development have all come together to create a recipe for disaster.

To his credit, California Governor Arnold Schwarzenegger has attempted to confront the problem. He has worked with the Federal Emergency Management Agency, US Army Corps of Engineers, and local emergency agencies to address the problem. In February 2006, the Governor declared a state of emergency and authorized immediate repair work. These stop-gap measures were followed by a $4 billion bond plan designed to fund levee repairs and flood-control projects. Beginning in 2007, DHS partnered with California to conduct a comprehensive review of the state's water system. The Department has also worked with the Army Corps of Engineers to design maps depicting where floodplains are located, so that appropriate restrictions on development can be instituted.

Unfortunately, these precautions triggered intense opposition from officials and businesses associated with local development. Recent articles in regional newspapers have underscored how county and local officials complained about the new flood maps and the requirement for elevated

construction in flood zones. The officials fear a residential or commercial building moratorium could result while new levees are being constructed. This unwillingness to delay economic benefit puts the entire population of this highly developed area at risk. It means that if a levee collapse was imminent, the consequences might be far graver than if prudent measures were expeditiously instituted to reduce the risk of flooding.

A second example concerns New Orleans and Hurricane Katrina. The cause of most of the damage to the city of New Orleans was the failure of a levee wall located at the 17th Street Canal. As the water in Lake Pontchatrain rushed back to the southern bank, it put an enormous amount of pressure on the canal that cuts through the city at 17th Street. The canal functioned as a funnel. Water surged into the canal, creating enormous hydraulic pressure, and the levee walls failed. Because of that failure a greater part of New Orleans filled like a bathtub.

Clearly, there were structural problems with how the levee was constructed. I was recently in New Orleans and went to the 17th Street Canal and examined the giant barrier that is now in place at the point where the canal meets the lake. The barrier allows the Army Corps of Engineers, if there is a sudden rise in the lake or a surge, to drop a massive steel gate that would hold back water entering the canal, preventing the kind of hydraulic pressure that caused the collapse of the levee wall three years ago.

The obvious question is why wasn't this barrier or a similar mechanism in place a decade ago? If it had been, then once Katrina hit, engineers would have taken immediate action and there would not have been a surge into the canal, the levee wall would not have failed, and the enormous loss of life and economic damage would have been averted. In fact, ten years ago, the Corps of Engineers proposed such a gate for the 17th Street Canal. It was vociferously opposed by local residents who felt it would spoil their view of the lake and by environmental groups concerned about effects on the area's ecology.

Private Enterprises and Communities

The Sacramento and New Orleans levees are examples of institutional failure to protect publicly owned resources and infrastructure. The nation should also examine this issue as it applies to privately owned enterprises upon which communities depend. Prime examples are the power and energy grids throughout America. Clearly, once a disaster occurs, restoring power

becomes critical. Without power, communities cannot deliver resources, evacuate people, or begin to rebuild. Almost every act depends on the ability to provide energy as rapidly as possible to the affected area.

This emphasis on the role of the private sector includes gasoline stations that provide the fuel that permits residents to get to the grocery store and other locations for necessities. When these facilities are unable to dispense fuel because of a lack of power, recovery efforts stall. This was a major problem in 2005 during hurricanes Rita and Wilma. That year, US Secretary of Energy Samuel Bodman and I wrote to the oil companies suggesting that they install generators at service stations. We outlined how critical these facilities were. Because of communities' reliance on service stations, the owners of these facilities have a responsibility to ensure that they can recover from the damage created by these disasters as quickly as possible. Unfortunately, the overall response to our initiative proved uneven at best. The state of Florida did pass a law requiring gas stations to have generators. But many other states failed to follow suit, and many companies have yet to provide their retail outlets with the capability to resume operation following a disaster.

From each of these examples, the same challenge emerges: Given the continuing problem of a crumbling or vulnerable infrastructure, how can government best ensure the infrastructure's protection and maintenance when faced with powerful and narrowly focused opposition? Given the political might of entrenched special interests, what can be done to ensure that the common good prevails? Certainly a cookie-cutter approach will not do. In addressing infrastructure vulnerabilities to terrorist threats, natural disasters, and aging, America needs to recognize there are several models available.

For maximum result, the nation needs to pursue a three-step process. Governments need to address the need for the protection and maintenance of infrastructure and facilities by utilizing a risk-based approach. That is the starting point not just for the federal government, but state and local governments also need to utilize the model designed to counter terrorist threats in their efforts to identify the critical infrastructure that is most vulnerable.

Second, federal agencies should examine the top 500 to 1,000 high-consequence and high-risk assets in their efforts to begin planning on how best to reduce vulnerabilities. If each state assessed its own infrastructure, the nation as a whole would have a better picture of the protection and

maintenance required to ensure continued functioning during natural disasters and emergencies. Once the most vulnerable assets are identified, a strategy for maintenance and protection can proceed. This strategy needs to estimate the cost of long-term maintenance on the existing infrastructure, and also whether further building should be limited in naturally vulnerable areas where the cost of protection to society far outweighs the benefit to a small number of individuals.

After this strategy is developed, it has to be funded, implemented, and continued for years to come. I have witnessed how worthy projects begin with a great deal of hoopla and public support, only to watch commitment wane once the television lights are off and the media moves on to the next issue. The plan to protect America's infrastructure and facilities cannot be executed in a week, month, or year. By definition, it is long-term in nature. It will require a sustained commitment and follow through, year after year, for generations to come. This approach is necessary if Americans want to protect their nation and their fellow citizens.

The bottom line: America's critical infrastructure will be in place well beyond the term of today's elected officials. It will outlast the normal politicking and funding conflicts that arise with every budget cycle. Now is the time to mount a long-term, comprehensive national strategy designed to preserve that infrastructure. We can build on the strategy already in place that guards against terrorist threats and apply that same disciplined approach to the challenges generated by nature and the passage of time. Now is the time for an active strategy based on all that America has learned from the past. By necessity this approach should be a partnership; but when necessary, it may require strong government action to minimize risk. This strategy should reflect a partnership committed to applying every tool available to the matter at hand.

In the end, planning is everything. The Gulf Coast evacuation during Hurricane Gustav succeeded because we had spent three years planning, building, and working to improve the system. Given a long-term focus on protecting and maintaining infrastructure, the nation will be able to rest in the knowledge that when the next catastrophe strikes, governments and industries had done all they could to protect life and property. We will have provided a service not just for this generation, but for those to come.