The Challenge of Protecting Critical Infrastructure

Philip AUERSWALD
Lewis M. BRANSCOMB
Todd M. LA PORTE
Erwann MICHEL-KERJAN

October 2005

Working Paper # 05-11

Center for Risk Management and Decision Processes – The Wharton School of the University of Pennsylvania
Jon M. Huntsman Hall – Suite 500 – 3730 Walnut Street – Philadelphia, PA 19104.6340 – USA
Phone: 215-898-1212 - Fax: 215-573-2130

The Challenge of Protecting Critical Infrastructure[1]

Philip AUERSWALD
School of Public Policy, George Mason University

Lewis M. BRANSCOMB
Kennedy School of Government, Harvard University

Todd M. LA PORTE
School of Public Policy, George Mason University

Erwann MICHEL-KERJAN[*]
The Wharton School, University of Pennsylvania

[1] This article is forthcoming in *Issues in Science and Technology* (U.S. National Academies and University of Texas at Dallas). This work is part of an ongoing joint initiative between GMU, Harvard and Wharton on protection of critical infrastructures that will result in a book to be published in the coming months by Cambridge University Press (contributors are leading experts, senior executives and federal officials).

[*] Emails: *auerswald@gmu.edu (Auerswald); lewis_branscomb@harvard.edu (Branscomb); tlaporte@gmu.edu (La Porte). Corresponding author (Wharton): Michel-Kerjan. Voice: 215-573-0515; email: erwannmk@Wharton.upenn.edu*

To deal with terrorist threats, the government must engage in more deeply rooted collaboration with the private sector.

In protecting critical infrastructure, the responsibility for setting goals rests primarily with the government, but the implementation of steps to reduce the vulnerability of privately owned and corporate assets depends primarily on private-sector knowledge and action. Although private firms uniquely understand their operations and the hazards they entail, it is clear that they currently do not have adequate commercial incentive to fund vulnerability reduction. For many, the cost of reducing vulnerabilities outweighs the benefit of reduced risk from terrorist attacks as well as from natural and other disasters.

The National Strategy for Homeland Security, released on July 16, 2002, reflects conventional notions of market failure that are rapidly becoming obsolete: "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. In these cases we should rely on the private sector." The Interim National Infrastructure Protection Plan (NIPP), released by the Department of Homeland Security (DHS) in February 2005, takes a similar position.

Although some 85% of the critical infrastructure in the United States is privately owned, the reality is that market forces alone are, as a rule, insufficient to induce needed investments in protection. Companies have been slow to recognize that the border is now interior. National defense means not only sending destroyers but also protecting transformers. In addition, risks to critical infrastructure industries are becoming more and more interdependent as the economic, technological, and social processes of globalization intensify. Just as a previous generation of policymakers adapted to the emergence of environmental externalities, policymakers today must adapt to a world in which "security externalities" are suddenly ubiquitous.

The case of CSX Railroad and the District of Columbia illustrates the tensions that have emerged over the competing needs for corporate efficiency and reduced public vulnerability to terrorist acts. Less than a month after a January 2004 train crash in South Carolina resulted in the release of deadly chlorine gas that killed 9 people and hospitalized 58 others, the District's City Council passed an act banning the transportation of hazardous materials within a 2.2-mile radius of the U. S. Capitol without a permit. The act cited the failure of the federal government "to prevent the terrorist threat." Subsequently, CSX petitioned the U.S. Surface Transportation Board (USSTP) to invalidate the legislation, claiming that it would "add hundreds of miles and days of transit time to hazardous materials shipments" and adversely affect rail service around the country. USSTP ruled in CSX's favor in March 2005, putting an end to the District's efforts.

Shortly after the decision, Richard Falkenrath, President Bush's former deputy homeland security advisor, highlighted in congressional testimony the severity of the threat that the act was intended to address: "Of all the various remaining civilian vulnerabilities in America today, one stands alone as uniquely deadly, pervasive, and susceptible to terrorist attack: toxic-inhalation hazard (TIH) of industrial chemicals, such as chlorine, ammonia, phosgene, methylbromide, hydrochloric and various other acids."

If industry itself is not motivated to invest in protection against attack and the federal government does not take the initiative, who will take responsibility for protecting chemical plants, rail lines, and other critical infrastructure? Who will make it harder for terrorists to magnify the damage of an attack by first attacking the infrastructure on which effective response depends? Who will ensure that these and other elements of the infrastructure are not used as weapons to kill or maim thousands of people in our cities? Is there, then, an adequate combination of private organizational strategies and public policies that will ensure reliable and resilient service provision in the long term? As the CSX case illustrates, consensus on how best to protect critical infrastructure has not emerged, despite the urgency created by terrorist threats, as well as the ongoing challenges of dealing with natural disasters. (*Editor's note: This article was completed before Hurricane Katrina struck the Gulf Coast*.)

An infrastructure is “critical” when the services it provides are vital to national security. The list of infrastructures officially considered critical is growing. In addition to the chemical sector, they are transportation, the defense industrial base, information and telecommunications, banking and finance, agriculture, food, water, public heath, government services, emergency services, and postal and shipping.

The threat of catastrophic terrorism has created a new relationship between national security and routine business decisions in private firms providing infrastructure services. Managers of these firms, like business managers elsewhere, are highly motivated to seek efficiency increases. The never-ending race for economy of scale and of scope and just-in-time processes that guarantee better results also leads to reduced redundancy, concentrated assets, and centralized control points. The new double-deck Airbus A380, the largest aircraft ever built, is designed to carry as many as 550 passengers in the quest for a decrease in the cost per passenger seat. More than half of the chickens destined for our supermarket shelves are processed by a handful of firms in Arkansas. Transformers used in primary power distribution have become so large that installations contain only one of them. The Internet is increasingly relied on for critical communications in the event of attack or disaster, not withstanding its well-known vulnerabilities to a variety of disruptions.

Before 9/11 and particularly since, much work has been directed at identifying vulnerabilities at the scale of individual firms, of industries, and more recently, of geographical regions. Many sound engineering-based proposals exist for reducing vulnerability. Large apartments and office towers can employ ventilation systems that detect and trap poisonous gases. Power distribution plants can better protect their largest transformers and store replacement units in safe places. Local governments can install LED traffic lights with trickle-charged batteries that will not fail during a blackout. Trains carrying toxic and explosive materials can be routed around cities. A 2002 National Academies study, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, contains other proposals to reduce vulnerabilities through the use of technology; subsequent work has added to the list. However, neither vulnerability assessments nor studies based on principles of engineering design address

the competitive pressures and other incentives that have led private firms to build infrastructures in their current forms.

Comprehensive public policy for critical infrastructure protection must begin with an understanding that "protection" per se should not be the goal. As a means of reducing vulnerability to attack at the regional or countrywide scale, it is minimally effective. In an open society, higher fences and thicker walls do little to reduce aggregate vulnerabilities. In many instances, protection simply shifts the focus of terrorists to other, less heavily fortified targets.

Even if one accepts the word "protection," what is being protected is not the infrastructure itself but the services it provides. With regard to terrorist threats, the policy goal should be to build capabilities for prevention of attacks that interrupt such services and for effective response and rapid recovery when such attacks do occur.

Sustainable policy must account for both the potential tradeoffs that exist at the firm level between efficiency and vulnerability and for the institutions and the incentives potentially affecting that tradeoff. Ultimately, policy must

- structure incentive systems for investment that enhance prevention of, response to, and recovery from the most likely and damaging attacks;
- ensure adequately robust internal operations of private firms, including greater system reliability for their services;
- limit imposed costs on firms to guarantee the competitiveness of our economy; and
- do all of the above in a manner that can be sustained by a complacent public with a short memory that may tire of the high costs and consumer inconvenience that government policies aimed at making critical industries less vulnerable may entail.

Although efficiency and vulnerability are produced jointly, they are not assessed together. A market economy routinely accounts for improved efficiency, because shareholders are always looking for the best return on investment in the short term.

However, vulnerability may be assessed only after it has been exposed by active study or system failure.

IF INDUSTRY ITSELF IS NOT MOTIVATED TO INVEST IN PROTECTION AGAINST ATTACK AND THE FEDERAL GOVERNMENT DOES NOT TAKE THE INITIATIVE, WHO WILL TAKE RESPONSIBILITY FOR PROTECTING CHEMICAL PLANTS, RAIL LINES, AND OTHER CRITICAL INFRASTRUCTURE?

Organizations are most likely to account for vulnerabilities that are linked to their own core activities. They will ignore equally serious consequences of attacks on, or attacks that employ, an infrastructure service that is assumed to be reliably available. Airlines, for example, have an inherent incentive to become intimately familiar with the factors that determine the risk of a crash. Beginning in the 1970s, airline managers were also compelled to systematically address hijacking threats. However, before 9/11, none were truly prepared for the possibility that passenger jets would be used as weapons of large-scale destruction.

Accountability for and accounting of vulnerabilities distant from core business activities are relatively uncommon, particularly when the perceived probabilities of occurrence are very low. Although economic incentives drive the accounting of core-business vulnerabilities, legal, organizational, and political dynamics drive the response to vulnerabilities that lie outside the core business concerns of any single firm or industry.

Traditional tools of risk assessment and risk management have become very sophisticated in recent years as a result of environmental, health, and safety regulations. Nonetheless, such tools remain largely inadequate in coping with high-impact, low-likelihood events. For many large technological network systems, the challenge of ensuring reliable operations has increased because operations both within and among firms have become increasingly interdependent. Elements of infrastructures in particular have become so interdependent that the destabilization of one is likely to have severe consequences for others.

As the scale and reach of these large technological systems have increased, the potential economic and social damage of failures has increased as well. The sources of such major disruptions lie in technical and managerial failures as well as natural disasters or terrorist attacks, as illustrated in the Northeast Blackout of August 2003. Economic and social activities are becoming more and more interdependent as well, so that the actions taken by one organization will affect others.

In this context, the incentives for any single organization to invest in prevention, response, and recovery are blunted. Without a global approach to understanding interdependencies and security externalities, determining the source of disruptions and quantifying the risk of such disruptions are difficult. Private decisionmakers will have neither adequate information nor adequate motivation to undertake investments that are more than justifiable from the standpoint of the system as a whole.

As terrorist attacks have emerged as potential threats to infrastructure, private-sector executives and policymakers must grapple with far greater uncertainties than ever before. This is particularly challenging because terrorists can engage in "adaptive predation," in which they purposefully adapt their strategies to take advantage of weaknesses in prevention efforts. In contrast, actions can be taken to reduce damage from future natural disasters with the knowledge that the probability associated with the hazard will not be affected by the adoption of these protective measures. The likelihood of an earthquake of a given intensity in Los Angeles will not change if property owners design more quake-resistant structures. The likelihood and consequences of a terrorist attack are determined by a mix of strategies and counterstrategies developed by a range of stakeholders and changing over time. This dynamic uncertainty makes the likelihood of future terrorist events extremely difficult (if not impossible) to estimate and increases the difficulty of measuring the economic efficiency of public policies and private strategies.

In that context, although private-sector actors can reduce system vulnerability by reducing dependence on vulnerable external services, decentralizing critical assets, decentralizing core operational functions, and adopting organization practices to improve resiliency, these organizations may face sanctions from markets for taking such actions if

they reduce efficiency, raise costs, or reduce profits. Indeed, markets rarely reward investments that reduce vulnerability to events so rare that there is no statistical basis for quantitative risk assessment.

Steering between market approaches that tend to remove system slack (increasing vulnerability to catastrophic system failure) and the redesign of private infrastructures to ensure more reliable functioning (though at higher cost to consumers), the federal government has generally opted for policies of partnerships between private-sector operators and government agencies. The Interim NIPP emphasizes the role of sector-specific agencies in coordinating private actors. The federal government also has overseen the development of a number of reliability regimes that involve combinations of government oversight and private-sector enforcement.

In both public/private and private/private partnerships, the tension between organizational autonomy and the independence of the constituent units of the large-scale system makes communication and coordination critical. When managers are not fully informed (or worse, are misinformed) regarding the actions and status of remote units, effective decisionmaking is not possible. Actions in one unit can have unintended and perhaps serious consequences elsewhere. Providing sufficient slack, encouraging constant and clear communications, and creating a consistent belief structure and safety-embracing culture help reduce this problem. Large-scale systems need to be flexible in adapting to rapidly changing situations.

Extraordinary levels of coordination of many organizations, public and private, will be required to secure any improved level of prevention, response, and recovery. Continuous but expensive organizational learning will be essential to producing an auto-adaptive response capability that will enable infrastructure service providers to deal more effectively with adaptive predators and dynamic uncertainty.

Yet such imperatives are unlikely to be tolerated by most private-sector organizations operating under normal business conditions, where bottom lines matter, where threats are difficult to discern, and where attacks are extremely infrequent. Sustaining watchfulness and the ability to deal with low-probability, high-impact events is the single most difficult policy issue facing critical infrastructure providers and homeland security agencies today.

Critical infrastructure protection needs to be understood as not only deploying a tougher exoskeleton, but also developing organizational antibodies of reliability that enable society and its constituent parts to be more resilient and robust in the face of new, dynamic, and uncertain threats.

Even though technological and managerial procedures may be in place to limit the occurrence of a devastating event and reduce its effects through resilient infrastructure, the possibility of suffering a large loss must still be seriously considered. Should that happen, the question of who should pay for the economic consequences is likely to take center stage. In the 2002 National Strategy, the White House considered recovery as a fundamental element of homeland security. In most developed countries, insurance is one of the principal mechanisms used by individuals and organizations for managing risk. Indeed, insurance is a key mechanism not only for aiding in recovery after an attack but also in inducing investments to make an attack less likely.

A well-functioning insurance market plays a critical role in ensuring social and economic continuity when large-scale disaster occurs. Private insurers paid about 90% of the $23 billion in insured losses that resulted from the four hurricanes that hit Florida in 2004. Two-thirds of the $33 billion in insured losses from the 9/11 attacks were paid by reinsurance companies (mostly European) that operate at a larger level worldwide. Because of the huge payouts, however, these companies either substantially increased their prices or stopped offering terrorism coverage altogether.

The collapse of the market for terrorism insurance after 9/11 motivated the passage of the Terrorism Risk Insurance Act of 2002 (TRIA). TRIA established a three-year risk-sharing partnership between the insurance industry and the federal government for covering commercial enterprises against terrorism for losses of up to $100 billion. Under TRIA, insurers are required to offer terrorism coverage to all of their commercial policyholders, who can in turn accept it or refuse to buy it. About 50% of firms nationwide purchased terrorism insurance in 2004. In case of an attack by foreign interests, the federal government would pay 90% of the insured losses above an insurer's deductible, providing free upfront reinsurance to insurers. The government can recoup *ex*

post part of its payment against all commercial policyholders, whether or not they bought terrorism insurance. The statute creating TRIA ends December 31, 2005, and it is not clear whether Congress will renew it in its current form, modify it, or let it go.

IN ADDITION TO ITS PRIME ROLE IN RECOVERY, INSURANCE CAN BE A POWERFUL TOOL IN INDUCING CRITICAL INFRASTRUCTURE INVESTMENTS THAT ENHANCE PREVENTION AND RESPONSE.

The *TRIA and Beyond* report, a detailed 10-month study by the Wharton School's Center for Risk Management in collaboration with a broad spectrum of public and private organizations, was released in August 2005. It concludes that TRIA "has provided an important and necessary temporary solution to the problem of how terrorism insurance can be provided to commercial firms," but does not constitute "an equitable and efficient long-term program and should be modified."

Routine government involvement in most catastrophic risk coverage programs (floods, hurricanes, earthquakes, and terrorism) is an implicit recognition of the necessity for the public sector to protect insurance infrastructure. Yet the respective roles and responsibilities of public and private actors in providing adequate protection to victims of terrorist attacks remain unclear. The creation by Congress or the White House of a national commission on terrorism risk coverage before permanent legislation is enacted, as urged by the Wharton team, would certainly help create a more efficient and equitable long-term solution that includes a necessary safety net for ensuring that insurance can play its traditional role in the recovery from major disasters or attacks involving critical infrastructure.

In addition to its prime role in recovery, insurance can be a powerful tool in inducing critical infrastructure investments that enhance prevention and response. As a third party between government and private firms, the insurance industry would play a key role in this domain. A firm or an individual investing in security and mitigation measures should be eligible to receive lower insurance rates. On the surface, the analogy to homeowner's insurance and hurricane and flood insurance, where this policy is prevalent, seems

compelling. But a closer look reveals that the potential role of insurance in inducing private investments in prevention and response is more red herring than silver bullet.

First, it is possible that having insurance will induce a manager to engage in riskier behavior than would have otherwise been the case—the moral hazard problem in insurance. Second, the link between the price of insurance and security/mitigation measures in the context of terrorism threats is tenuous at best. The current evidence is that almost none of the insurers providing coverage for terrorism in the United States have thus far linked in any way the price of coverage to the security measures in place. Why is this the case? The significant decrease in the price of terrorism insurance four years after 9/11, combined with the relatively high price for reinsurance (when available), does not provide a large window for price reduction. Perhaps more important, the dynamic uncertainty due to adaptive predation by terrorists makes it extremely difficult to measure and to price the efficiency of any security measure. Without a price, there cannot be a market.

Enhancing capabilities in the United States for prevention, recovery, and response relating to attacks on critical infrastructure will not be easy. In the long term, responding to this challenge will not only require changes in the technologies and structures adopted by threatened firms. It will also require improving the effectiveness of private strategies and public policies, reflecting an emerging balance of public and private roles and responsibilities.

Institutional capabilities to identify, negotiate, and implement such policies are at least partly in place. The union of 22 federal bodies under the umbrella of the new DHS, along with the current reform of the intelligence services, is the most significant federal reorganization of the past half-century, although DHS has yet to give priority to addressing the vulnerability of critical infrastructures. The transformations induced by the corporate trust crisis and the new Sarbanes-Oxley era are also changing how most firms operate, but it is unclear that the changes taking place will add anything to counterterrorism capability in private industry. Finally, for the general public, an

important issue will be willingness to sacrifice for security, whether through higher prices and taxes or through loss of freedom and privacy.

Beyond infrastructure vulnerability assessments, continuity of operations planning, and deliberate investment in a small set of obviously cost-effective technologies, the following structural, organizational, and financial strategies should be considered to improve the capacity of the critical infrastructure service providers and public authorities to perform their functions:

- strike a balance between strategies that emphasize anticipation (reducing the likelihood of attack) and those that emphasize resilience (reducing the damage resulting from attack);
- recognize and support high-reliability organizations and reliability professionals;
- enhance the capabilities of autoadaptive response systems of various types;
- reward information-sharing about technological and organizational changes and encourage organizations to emphasize safety;
- promote dialogue among citizens and stakeholders to define priorities and explore options for action; and
- develop incentive programs to induce private investment in security by relying on market forces to the extent possible.

Strategies to protect critical infrastructure are not viable unless they are politically and economically sustainable. Sustainability may be enhanced by a deliberate policy of seeking win-win options that promise public and private benefits beyond vulnerability reduction. Public relations, reputation, and the possibility of tort liability may motivate some firms to invest even without additional government pressure. Understanding the motives, constraints, and capabilities of potential attackers may inform decisions regarding investments in prevention, response, and recovery.

The challenge of critical infrastructure protection is a multifaceted one requiring a variety of responses. Market mechanisms and engineering design both have roles, but neither is sufficient. As national security increasingly finds its way into the boardrooms of U.S. corporations, rigid and limited public/private partnerships must give way to flexible, more deeply rooted collaborations between public and private actors in which trust is developed and information is shared. By directly addressing at an operational level the potential tradeoffs between private efficiency and public vulnerability, such collaborations will lead to better, if not definitive, solutions.

Recommended reading

Center for Risk Management and Decision Processes, *TRIA and Beyond*. *Terrorism Risk Financing in the U.S. (*Philadelphia, PA: The Wharton School, University of Pennsylvania, August 2005).

National Academies, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*,Committee on Science and Technology for Countering Terrorism, Lewis M. Branscomb and Richard Klausner, co-chairs (Washington, DC: National Academies Press, 2002).