

# Holistic Strategy for Urban Security

Richard G. Little<sup>1</sup>

---

**Abstract:** Since September 11, 2001, the vulnerabilities to terrorism of our urban areas, and how best to address them, have been subject to considerable discussion, debate, and reflexive defensive measures. Although direct physical responses to such frightening events are certainly understandable, they are not based on a true assessment of risk, nor do they necessarily represent an effective, let alone cost effective, approach to addressing the threat of urban terrorism. This paper will explore recent trends in physical protection and offer observations on a rational basis for evaluating security strategies; some alternative, nonstructural approaches to urban security, and the need for robust institutions with well-qualified people in critical positions to develop and implement these strategies. It will seek to demonstrate that a holistic strategy that incorporates technology, people, and institutions will achieve far greater long-term security as well as possible ancillary mitigation benefits from other hazards.

**DOI:** 10.1061/(ASCE)1076-0342(2004)10:2(52)

**CE Database subject headings:** Security; Terrorism; Urban areas; Blast effects; Risk management; Hazards.

---

## Introduction

Since September 11, 2001, the vulnerabilities to terrorism of our urban areas, and how best to address them, have been subject to considerable discussion, debate, and reflexive defensive measures. Armed guards and concrete barriers appeared almost immediately after the terrorist attacks. Blast-resistant construction features, once the province of military installations and critical government facilities, are increasingly being considered for commercial buildings (Lipton and Glanz 2002; MCEER 2002), as are changes to building codes (City of New York 2003). Systems to detect and interdict chemical and biological agents are also under development to protect cities and their occupants from the effects of an attack utilizing these weapons (Miller 2003). Although direct physical responses to such frightening events are certainly understandable, they are not based on a true assessment of risk, nor do they necessarily represent a comprehensive approach for addressing the threat. In fact, given the large number of assets to protect in even a moderate-sized city and their widely dispersed locations, relying solely on physical measures to thwart or blunt an attack may not be an effective, let alone cost-effective, approach to addressing the threat of urban terrorism. This paper will explore recent trends in physical protection; offer observations on a rational basis for evaluating security strategies; give some alternative, nonstructural approaches to urban security; and discuss the need for robust institutions with well-qualified people in critical positions to develop and implement these strategies. It will seek to demonstrate that a holistic strategy that incorporates technology, people, and institutions will achieve far greater long-term security as well as possible ancillary mitigation benefits from other hazards.

## Cities and Their Vital Systems

Throughout history, cities have been the locus of enormous economic, social, and political activity, supported and enhanced by the services provided by their infrastructures (NAE 1986). If we think of infrastructure as the delivery vehicle for the totality of services necessary to support these activities, the definition of *infrastructure systems* must include institutions and people as well as pipes, pumps, cables, switches, and the like (Little 1999). Because of this, the challenge of ensuring the continuity of vital services in the face of terrorism and other hazards is more complicated than just the protection of physical assets.

Typically, hazard mitigation strategies for infrastructure have generally addressed first-order effects—designing robust systems to resist extreme loads imparted by natural events or malevolent acts such as sabotage and terrorism. However, because these systems do not operate independently, strengthening a single system is seldom effective in preventing outages. For example, following the 1995 Kobe earthquake, in addition to adequate water supply not being available, the communication and transportation systems also failed, making an effective response by fire services impossible (MCEER 1995).

Urban infrastructures are inherently interconnected and particularly vulnerable to cascading-type failures from a single event (Little 2002a), which also makes them difficult to strengthen effectively (Gilbert et al. 2003). The consequences of this type of cascading failure of interdependent systems in an urban environment were almost experienced following the World Trade Center attacks of September 11. The collapse of the World Trade Center towers caused extensive damage to the slurry wall or “bathtub” that surrounded the buildings’ deep basements (Tamaro 2002). Had the slurry wall failed, the likely outcome would have been disastrous—the possible flooding and massive disruption of a large portion of New York’s underground rail transit system on which the City depends so heavily:

The PATH tubes were century-old cast-iron structures, probably brittle in places, and now at immediate risk of failure. If either of them broke catastrophically, the Hudson River would flood into the foundation hole, filling it at high

---

<sup>1</sup>Director, Board on Infrastructure and the Constructed Environment, National Research Council, 500 5th St., NW, Washington, D.C. 20001.

Note. Discussion open until November 1, 2004. Separate discussions must be submitted for individual papers. To extend the closing date by one month, a written request must be filed with the ASCE Managing Editor. The manuscript for this paper was submitted for review and possible publication on August 14, 2003; approved on December 8, 2003. This paper is part of the *Journal of Infrastructure Systems*, Vol. 10, No. 2, June 1, 2004. ©ASCE, ISSN 1076-0342/2004/2-52-59/\$18.00.

tide to a level just five feet below the street, and drowning unknown numbers of trapped survivors. Moreover, on the far side of the river, a wall of water would flood the Jersey City station, and from there, via connecting rail links, would circle uncontrollably back into Manhattan, rush through the passages beneath Greenwich Village, and take out the West Side subways from the southern tip of the island nearly to Central Park. Vulnerability to sequential flooding was a known weakness of the PATH system, and it had been highlighted in a report circulated discreetly among government officials after the earlier World Trade Center attack: The parking-garage bombing of February 23, 1993. But maybe because such flooding was also something of an apocalyptic vision—and therefore somehow unreal—no defenses were erected against it (Langewiesche 2002).

One lesson that must be learned from the attacks of September 11 on the World Trade Center and the Pentagon is that iconic structures—symbols of the cultures that support them—will continue to be likely targets of terrorism (Rypkema 2003). So long as the roots of such terrorist attacks continue to exist, our cities and their important structures must be considered at risk. Protective technologies can address some but not all of this risk.

### Physical Protection Strategies

Historically, cities provided security to people in times of unrest and conflict. Until modern explosives and aerial bombardment rendered them moot, most physical protection strategies for cities and towns were aimed at keeping an attacker at bay by means of moats, walls, and other physical obstacles. Even today, standoff (the distance between a bomb and its intended target) is still considered the most effective defense against a terrorist vehicle bomb, because blast energy falls off with the cube of the distance and dissipates very quickly. However, when effective standoff distance is not available or cannot be enforced, other measures are available to protect targeted buildings from bomb damage.

The numerous terrorist bombing attacks experienced in the past 25 years have generated considerable research into the effects of bomb blasts on buildings and people (NRC 2000). As a result, the vulnerabilities of buildings to deliberately placed bombs are reasonably well understood, as are the relative effectiveness of various countermeasures (Little 2002b). Blast-resistance in buildings is generally provided by passive features such as additional reinforcement and connections in the structural frame for increased ductility, composite fiber wraps to prevent shattering of columns and slabs, and high-performance glazing materials that resist blast pressures (AMPTIAC 2003). When such structurally enhanced buildings have been attacked, these measures have been shown to be quite effective in reducing damage and casualties (Mlakar et al. 2003). These features may also provide some collateral benefits against natural hazards such as earthquakes and extreme winds. However, beyond a possible local deterrent effect, these features do nothing to protect nearby buildings that have not been so enhanced.

Similar tactics are also being considered for defending buildings against biological and chemical weapons by employing active sensor and control systems (DARPA 2003). In theory, if a chemical or biological attack were to occur, sensors would detect, identify, and classify the agent. Instructions would then be transmitted to control actuators that would then direct a response by the building systems. One possible response would be to shut

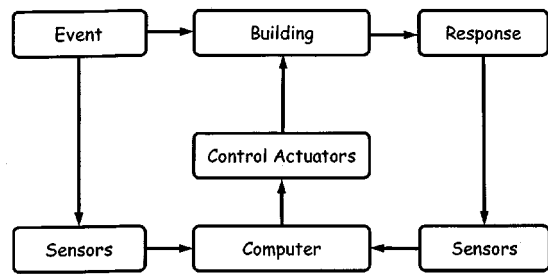


Fig. 1. Logic for typical smart building control system [after Spencer (2002)]

down all the air intakes and reverse flow on the HVAC (heating, ventilation, and air conditioning) system to purge the building to the atmosphere. The system would monitor building conditions in a continuous feedback loop until the threat had been neutralized. Fig. 1 is a schematic diagram of a prototypical system for this type of active building control.

Because sensors continue to improve through active research programs in several government agencies (e.g., NSF, DARPA) and “smart” building controls have been available for some time, the technology is generally available to deploy such systems. However, beyond applications in what might be termed “boutique buildings,” their potential for widespread implementation may be very limited. First, there is the underlying assumption that this technology can be deployed effectively—it presumes that the sensors can sense what they need to and nothing more, and that the actuators can be programmed to know when and what to actuate and to do so quickly, minimizing both Type I and Type II errors. However, the American Society of Heating, Refrigeration, and Air Conditioning Engineers has noted that an active response (i.e., shut down and purge) may not be the best course of action when an attack is suspected to have occurred (ASHRAE 2003). Second, the cost of such systems [estimated to be in the range of \$10<sup>5</sup> to \$10<sup>6</sup> per building (Harvey Ko, Applied Physics Laboratory, Johns Hopkins University, personal communication, 2003; Kathleen Paulson, Naval Facilities Engineering Services Center, personal communication, 2003)], weighed against their potential benefits for widespread risk reduction, may prove to be excessive. As was also the case for blast-mitigation features, these systems do nothing to reduce the vulnerability of nearby, unprotected buildings. In fact, purging a contaminated building to the atmosphere may put more people at risk outside of the “protected” building than were subject to the initial attack.

### Limits of “Protective” Technology

History is littered with accounts of allegedly foolproof or failsafe protective technologies that failed spectacularly when tested. The “unsinkable” *Titanic* and the “impregnable” Maginot Line added new terms to the lexicon of failure. Their designers assumed what was believed to be a rational threat scenario, then planned and designed for it, yet both failed utterly in practice. The damage limits for the *Titanic* turned out to have no basis in reality—the iceberg that damaged the ship did not know that the design assumed that only a certain number of compartments could be compromised. More to the point in the current discussion of urban

terrorist attack, in World War II, the Germans simply chose not to confront the extremely formidable defenses on the French border and attacked through lightly defended Belgium instead. Recent studies suggest that, when confronted with formidable defenses, terrorists may readily substitute more vulnerable targets (Enders and Sandler 2004). However, a questionable reliance on protective technology continues to the present day. The Karpun tunnel fire in Austria that claimed 155 lives in 2000 started in a train believed to be fireproof. An assessment of the event noted;

In November 2000, a supposedly “fireproof” train in a tunnel in the Austrian Alps caught fire and led to the deaths of 155 people. While many factors contributed to the disaster, one of them was thinking that a vehicle can be fireproof (Carvel 2002).

## Learning from Failure

Strategies for hazard mitigation, including hazard-resistant design for structures and other engineering works, has improved continuously from the observation of past failures, assessment of their causes, and improvements in techniques and materials (Petroski 1992, 1994; NRC 1994; Mileti 1999) However, despite the value of this forensic approach to the advancement of practice, it has very real limits. This is partially due to the emphasis on identifying *causes* and determining who was at fault rather than *preventing* future failures. In a recent study of errors in the health care industry, the Institute of Medicine noted that there are major conceptual concerns with commonly used forensic techniques in medicine:

The complex coincidences that cause systems to fail could rarely have been foreseen by the people involved. As a result, they are reviewed only in hindsight; however, knowing the outcome of an event influences how we assess past events. *Hindsight bias* means that things that were not seen or understood at the time of the accident seem obvious in retrospect. Hindsight bias also misleads a reviewer into simplifying the causes of an accident, highlighting a single element as the cause and overlooking its multiple contributing factors. Given that the information about an accident is spread over many participants, none of whom may have complete information, hindsight bias makes it easy to arrive at a simple solution or to blame an individual, but difficult to determine what really went wrong. (IOM 2000).

Kletz, in a study of industrial accidents, also cautions about too much emphasis on causes:

If we talk about causes, we may be tempted to list those we can do nothing about. For example, a source of ignition is often said to be the cause of a fire. But when flammable vapor and air are mixed in the flammable range, experience shows that a source of ignition is liable to turn up, even though we have done everything possible to remove known sources of ignition. The only really effective way of preventing an ignition is to prevent leaks of flammable vapor. Instead of asking, ‘What is the cause of this fire?’ we should ask ‘What is the most effective way of preventing another similar fire?’ We may then think of ways of preventing leaks (Kletz 2001).

This suggests that care needs to be taken in analyzing past failures so that proposed solutions address the real issues, not merely the obvious ones. For example, in the aftermath of September 11, there has been much public demand to change building code provisions regarding structural collapse. However, the

connection between airplane impact and the collapse of the World Trade Center, although valid, gets caught in Kletz’s “obvious cause” trap and rather misses the point. Instead of asking “How can we design buildings so that they will not collapse if deliberately struck by an airplane?” perhaps the more appropriate question is “How can we protect tall buildings from similar attacks?” The answer to the second question lies at least as much with airport security as with structural design and building codes. Following Kletz’s admonition, perhaps the real question is not “What are the best technologies to resist terrorist attack?” but rather, “How can we reduce casualties in the event of an attack?”—a fundamentally different question.

## Risk and Security

Although governments and other stewards of the public welfare have a clear responsibility to provide for the safety of those entrusted to their care, when considering protection levels for the safety of buildings and infrastructure, the government must also consider the cost of providing that level of safety. Ultimately, a choice must be made whether an investment to reduce risk to those directly affected is of greater benefit to society than expending the funds for some other purpose (NRC 1985).

One way to express risk conceptually is as the probability of an adverse event multiplied by the consequences of that event, or  $R = P \times C$ . The assessment of that risk can be defined by three questions (Kaplin and Garrick 1981):

- What can go wrong?
- What is the likelihood that it would go wrong?
- What are the consequences of failure?

These questions are relatively straightforward, but in practice they often prove difficult to define precisely, particularly when assessing environmental or health consequences. Because of this, a “precautionary principle” has emerged whose basic tenet is that, when an activity raises threats of harm to the environment or human health, precautionary measures should be taken even if some cause-and-effect relationships are not fully established scientifically. Three versions of the precautionary principle have been described (Wiener and Rogers 2002):

- Lack of full scientific certainty about a risk shall not justify postponing an action to prevent it.
- Uncertainty about a risk justifies action to prevent it.
- The proponent of an activity posing uncertain risk bears the burden of proving that the activity poses “no” or an “acceptable” risk before the activity can go forward.

In any case, the key element of the precautionary principle is that it incites us to take anticipatory action in the absence of scientific certainty. Although this might suggest that reflexive, postattack security enhancements around public buildings and spaces are quite reasonable, the precautionary principle actually provides little useful input to decision making when compared to quantitative risk analysis (i.e., benefit/cost/risk assessment), which offers insights into the likely consequences of a proposed action. This shortcoming has been highlighted by Starr in a recent critique of the precautionary principle (Starr 2003).

Risk management builds on the risk-assessment process by seeking answers to a second set of questions (Haimes 2002):

- What can be done and what options are available? (What is the mix of site selection and configuration, building features, and management practices that will provide the desired level of protection?)
- What are the associated trade-offs in terms of all costs, ben-

efits, and risks? (For example, increased cost normally would be traded off with reduced risk and improved confidence in security.)

- What are the impacts of current management decisions on future options? (Policy options that seem cost-effective at present must be evaluated under plausible future changing conditions. For example, providing certain physical hardening may preclude building modifications to increase functionality in the future.)

These questions are particularly relevant to the current discussion because experience has shown that all too often, “temporary” security measures become de facto permanent solutions (NRC 2003)—in effect, a precautionary approach to the possibility of future attacks without further discussion or assessment of risk, costs, or benefits. This is because physical protective features typically target generic vulnerabilities and are not generally selected based on a quantified (even if somewhat subjective) risk calculation.

Given the high cost of implementing an effective urban physical security strategy, the participation and knowledge of all affected parties, including policymakers, law-enforcement officials, building owners and occupants, planners, architects, engineers, and security specialists will be required. Much of the current debate on security in an open society is unproductive because some believe that risk must be minimized regardless of the consequences for design or accessibility while others demand attractive, accessible architecture with minimal concern for security. This debate fails to recognize the distinct difference between the scientific calculation of risk on the one hand, and community value judgments that must be incorporated on the other. Social judgment theory provides an interesting and useful way to frame this complex and often emotionally charged discussion (Kleindorfer et al. 1993) In any event, questions of this type are not for engineers to answer alone (NIST 1999).

### A Rational Basis for Urban Security

Protecting buildings and those they shelter from terrorist acts may be viewed within a basic systems framework that seeks to prevent, mitigate, and respond to future attacks (Sevin and Little 1998). This framework complements the graded approach to protecting buildings from attack developed by Mays and Smith (1995). Their approach, which incorporates five steps of increasing complexity and cost, seeks to accomplish the following objectives:

- *Deflect* a terrorist attack by showing, through layout, security, and defenses, that the chances of success for the terrorist is small; targets that are otherwise attractive to terrorists should be made anonymous.
- *Disguise* the valuable parts of a potential target, so that the energy of attack is wasted on the wrong area and the attack, although completed, fails to make the impact the terrorist seeks; it is reduced to an acceptable annoyance.
- *Disperse* a potential target, so that an attack could never cover a large enough area to cause significant destruction, and thereby, impact; this is suitable for a rural, industrial installation, but probably unachievable for any inner-city building.
- *Stop* an attack from reaching a potential target by erecting a physical barrier to the method of attack; this covers a range of measures from vehicle bollards and barriers to pedestrian entry controls. Against a very large car bomb, in particular, this is the only defense that will be successful.

		Consequence			
		Catastrophic 1	Very serious 2	Serious 3	Not serious 4
Likelihood	Certain A	1A	2A	3A	4A
	Highly probable B	1B	2B	3B	4B
	Probable C	1C	2C	3C	4C
	Improbable D	1D	2D	3D	4D

Risk Level	Action Indicated
1A,1B,1C,2A,2B,3A	These are unacceptable risks. Action must be taken to eliminate or reduce them.
1D,2C,2D,3B,3C	These may be unacceptable risks. These risks may be acceptable as part of a comprehensive risk management strategy.
3D,4A,4B,4C,4D	These risks are usually acceptable as part of a comprehensive risk management strategy.

Fig. 2. Probability/consequence matrix for evaluating risk levels

- *Blunt* the attack once it reaches its target, by hardening the structure to absorb the energy of the attack and protect valuable assets.

Fig. 2 is a simplified decision matrix that categorizes possible actionable outcomes of the risk assessment process based on the relative probabilities of certain classes of events and their consequences and permits rational choices to be made to address them. Predictably, high-probability events with adverse outcomes demand priority attention. Although this is useful information, it provides little insight into what countermeasures might be most appropriate in a specific application. In the case of protection from vehicle bombs, the action taken may be to acquire additional land for standoff, provide hardening features, limit vehicular access and parking, or assign security personnel to patrol the area. It could even entail relocating personnel and operations to another location. These decisions can be based on a probability of attack defined by decision makers and based on their individual circumstances; e.g., “highly probable” from the risk matrix may be  $10^{-1}$ /year for one and  $10^{-3}$ /year for another. Consequences, in human and economic terms, could be defined as “catastrophic,” meaning total building destruction and great loss of life, to “not serious,” representing little or no damage and only minor injuries. Other, similar definitions could also be used but categorization is essential to a common understanding of the risk and the strategy for managing it. Once definitions have been selected and accepted, they can not be adjusted unilaterally. Potential countermeasures can then be evaluated objectively based on their cost, ability to implement, and effectiveness. Comprehensive security strategies can be developed based on realistic estimates of risk for a specific facility or location and not just as precautionary measures based on the vulnerability of buildings to a certain type of attack. This approach can also be used to assess and update security measures as better information becomes available or risk tolerance changes. Marshall (2002) has developed a life-cycle economic model to help choose financially responsible strategies that reduce the expected value of terrorist-induced damages and which could be coupled with a risk management model. However, al-

though theoretically straightforward, there is, as of yet, a paucity of data to support a convincing calculation of costs and benefits.

In another approach, Gale and Husick (2003), likening the protection of critical infrastructure systems to the “commons” of the environmental movement—a vital asset shared by all but owned by none that is ultimately laid waste because it is in everyone’s individual best interest to take much while contributing little to its stewardship—have proposed a “security impact statement” as a decision-making tool for societal investments in protecting the commons. Their proposal would allow for the comparison of a full range of options from purely technological to more balanced systems that rely on institutions as well. This type of assessment would be helpful in determining the true value, in terms of the costs and benefits to society, of plans to protect assets individually versus broader strategies that might address multiple hazards in many locations.

The “good of the commons” approach is reinforced by a lesson from both world wars. Until the convoy system was introduced in 1917, Great Britain was in real danger of being forced out of the war because of the enormous shipping losses inflicted by German submarines (Padfield 1995). Even though the speed of a convoy was restricted to that of the slowest ship, it was far simpler to protect a large group of slow ships with a few escorts when compared to the nearly impossible task of protecting the same number of ships sailing alone on different routes and at different speeds. After experiencing devastating losses to German submarines early in World War II, the convoy system was again instituted and trans-Atlantic shipping routes were preserved. This suggests that it may be more effective (and economical) to think of urban security in neighborhood or district terms rather than as protecting individual buildings. For example, restricting trucks from parts of the city at certain times of the day, or requiring a physical inspection (or explosives detection screening) before they could enter, would initially be disruptive and probably costly. However, it would be a far greater deterrent to terrorist attack than merely providing enhanced construction features to a few buildings. If nothing else, it provides an alternative strategy against which the cost and effectiveness of hardening individual buildings can be compared.

### The Importance of Institutional Resilience

The World Trade Center attacks provide some interesting lessons for a more comprehensive approach to urban security. Several reconnaissance-level studies of the performance of infrastructure in the vicinity of the World Trade Center in the days and weeks following the attacks (Tierney 2002; Zimmerman 2002; Wallace et al. 2003) all underscore the notion that resilience or the ability to recover quickly is a critical feature of survivable systems. Resilience is often provided by means of increased robustness, which increases failure-resistance through design and/or construction techniques, or redundancy, which provides duplicative capacity for service delivery. It will be shown that these characteristics are just as critical for institutions as for the physical systems themselves.

New York City was able to recover relatively quickly (compared to how other cities might have fared) after September 11 not only because of the inherent redundancy of its physical infrastructures (which is considerable) but because of its institutional resilience as well. Many of the service providers involved in New York’s recovery (e.g., Consolidated Edison, Verizon, AT&T, MTA) possessed considerable capacity in people who are consid-

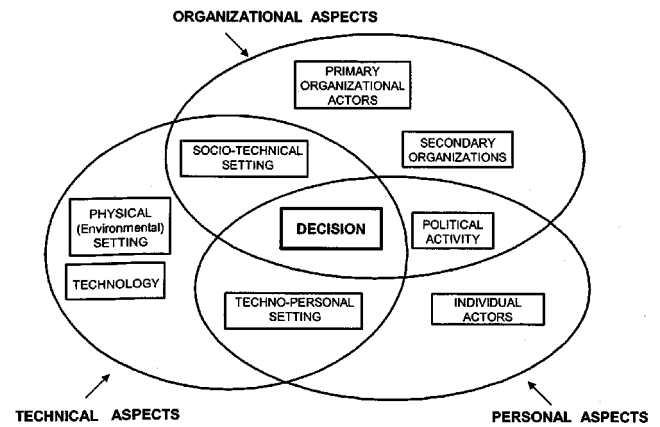


Fig. 3. Sociotechnical system model for decision making

ered international experts in their fields; state-of-the-art equipment and configuration management; as well as other physical and institutional resources necessary to effect recovery (O’Rourke et al. 2003). It is not apparent that leaner, less robust systems would have performed as well and, as a result, it is likely that recovery would have been hampered.

Petak (2003) recently made a strong case for the need for a holistic approach to implementing earthquake mitigation measures that applies here as well. He noted that mitigation technology has advanced considerably over the years but deployment has not kept pace, even in earthquake-prone California. He believes one of the principal reasons for the gap is that earthquake risk reduction is viewed by many as a *technical* problem with a technical solution. However, despite the value of technology, it requires institutions and people to develop and implement a workable, sociotechnical systems solution. Perrow (1999) also highlights the importance of people as “circuit breakers” in critical systems, and Schneier (2003) champions their role in openly evaluating security measures. Fig. 3 is an illustrative model of sociotechnical systems that has been developed by Linstone (1984) and is very useful for visualizing the interactions that occur during a complex decision-making process. Developing a successful strategy for urban security requires that these interactions be understood and enabled by all involved stakeholders. Security will be neither holistic nor effective if it is restricted to narrow professional or disciplinary stovepipes or if interactions among government officials, security professionals, program and financial staff, and emergency responders occur only on a project-by-project basis. Robust and effective security will require that dialogues be initiated and sustained between and among the various stakeholders using terms of reference that all can relate to and act upon. The Department of Homeland Security, through FEMA, is disseminating valuable guidance documents in this area and could play a key role in fostering and maintaining these interactions (FEMA 2003a,b).

Despite the importance of institutions for developing and implementing balanced security and emergency response strategies, in the post-September 11 timeframe many of our critical institutions are just emerging from years of neglect and crisis. Garrett (2000) has painted a grim picture of how, in the 20th century, the public health infrastructure in the United States deteriorated from a formidable first-line defense against infectious disease to a struggling, underfunded, and underappreciated appendage. Today, as we struggle to develop and deploy technologies to combat bioterrorism, citizens and policymakers alike are

wondering if the United States is capable of dealing with deliberately induced outbreaks of infectious disease. However, terrorism is not the only threat. The recent SARS outbreak demonstrated that the global economy and worldwide air transportation network have created the closely coupled system that Garrett speculated would make it possible, and even likely, that someone infected with a highly contagious disease would unwittingly spread the infection far beyond their borders. Fortunately, the initial assessments of the worldwide response to SARS demonstrated that there is hope that the global public health networks are again becoming functional and effective (Drazen 2003).

There are also other notable cases of recent institutional breakdown. In 1 week in July 1995, excessive heat in Chicago caused 739 deaths—more than Hurricane Andrew, the crash of T.W.A. Flight 800, the Oklahoma City bombing, and the Northridge, California, earthquake combined. Klinenberg (2002), documenting this event in what he termed a “social autopsy,” cited five primarily institutional factors that he believes contributed to the enormity of the disaster:

- Delegation of key health and support services to paramilitary (i.e., police and fire) organizations;
- Lack of an effective system for organizing and coordinating city, county, state, and federal agencies;
- Lack of public will or ability to provide basic resources for those in need of support;
- Expectation that urban residents will respond as “smart consumers” of public services; and
- The increasing role of public relations, as opposed to real response, in managing crises.

By any definition, this was an extreme climatological event, and breakdowns in the electrical and water distribution systems certainly contributed to its severity. However, the magnitude of its consequences, particularly among those disconnected from the social and economic mainstream, was clearly exacerbated by the failure of public institutions to protect those who needed them the most. Klinenberg attributes part of this breakdown to pressures to “make government more like a business.”

The momentum to privatize and streamline formerly public services, and its possible consequences, has been noticed at the highest levels of government. The director of the Office of Science and Technology Policy, in testimony before the United States Congress, noted that:

- Deregulation and growth of competition in key infrastructures has eroded spare infrastructure capacity that formerly served as a useful shock absorber; and
- Mergers among infrastructure providers have led to further pressures to reduce spare capacity as management has sought to wring out excess costs (Marburger 2002).

## Towards a Holistic Approach to Urban Security

Unfortunately, we find ourselves in a time where former contexts of threat, vulnerability, and target have all changed and continue to do so. Threats are unpredictable and the full range of threats probably unknowable. We will never be able to anticipate all possible threats and even if we could, there is not enough money to deploy technologies to address them. Security in this situation needs to be flexible and agile and capable of addressing new threats as they emerge. Protective technologies have a key role to play in making our cities safer but only if supported by the organizations and people who can develop preattack security strategies, manage the response to an attack, and hasten recovery from

it. Investments in emergency response technologies, strategies, and organizations have the potential to be particularly cost-effective because they are not tied to a place or event. The ancillary benefits from investments in this type of holistic approach are that these organizations and people will also be available to deal with natural disasters or other, yet unanticipated, crises should they occur. Single-purpose protective technologies will only be effective if the threat and design intersect. Otherwise they will constitute a formidable but ineffective defense—a sort of modern-day Maginot Line. On the other hand, well-designed and maintained infrastructure systems are likely to recover as quickly following an earthquake, landslide, or flood as a terrorist attack, as well as providing better service over their lifetimes.

The tragic events of September 11 made it abundantly clear that there are some scenarios for which direct defense is neither practical nor realistic and that it is difficult, if not impossible, to prevent destructive acts by persons unconcerned with their own safety or survival. Therefore, preventing an attack, facilitating rapid rescue and recovery of victims, and restoring vital services in the aftermath of an attack must be key components of an urban security strategy. A comprehensive solution to the risks of terrorism goes far beyond this paper (NRC 2002; Wulf et al. 2003), but we possess, and can employ, appropriate techniques, technologies, and institutions to implement a sensible and effective response to terrorism directed against our cities.

The importance of sustained strategic investment over a broad front that includes both technology and institutions cannot be overstated. Shortly after the terrorist attacks of September 11, the economist Paul Krugman noted that the laxity of airport security had been an issue for years while calls to fund a professional, high-quality service had gone unheeded (Krugman 2001). He ascribed this largely to a national culture that was unwilling to pay the price of public safety and which up until September 11 was willing to depend on private companies to do a job that probably belonged in the public domain all along. He drew a parallel to the decay of the public health infrastructure in the United States described by Garrett and concluded with an observation that remains germane to this discussion: “If we continue to nickel-and-dime crucial public services, we may find—as we did last week—that we have nickel-and-dimed ourselves to death.”

## Acknowledgment

The writer is deeply indebted to William A. Wallace of Rensselaer Polytechnic Institute, who reviewed an early draft of this paper and provided many valuable comments and suggestions.

## References

- Advanced Materials and Processes Technology Information Analysis Center (AMPTIAC). (2003). “Protecting people at risk: How DoD research reduces the impact of terrorism.” *The AMPTIAC Quarterly*, 6(4).
- American Society of Heating, Refrigeration, and Air-Conditioning Engineers (ASHRAE) (2003). *Report of Presidential Ad Hoc Committee for Building Health and Safety under Extraordinary Incidents on risk management guidance for health, safety, and environmental security under extraordinary incidents*, Atlanta.
- Carvel, R. (2002). “The history and future of fire tests.” *Tunnels Tunnel. Int.*, 11, 34–35.

- City of New York. (2003). *New York City Department of Buildings World Trade Center Building Code Task Force, findings and recommendations*, Dept. of Buildings, New York.
- Defense Advanced Research Projects Agency (DARPA). (2003). "Immune building program." (<http://www.darpa.mil/spo/programs/immunebuilding.htm>) (Aug. 5, 2003).
- Drazen, J. M. (2003). "SARS—Looking back over the first 100 days." *N. Engl. J. Med.*, 349(4), 319–320.
- Enders, W., and Sandler, T. (2004). "What do we know about the substitution effect in transnational terrorism?" *Terrorism research*, A. Silke, ed., Frank Cass, London, in press.
- Federal Emergency Management Agency (FEMA). (2003a). "Reference manual to mitigate potential terrorist attacks in high occupancy buildings." *FEMA 426*, Washington, D.C.
- Federal Emergency Management Agency (FEMA). (2003b). "Primer for design of new buildings to mitigate terrorist acts." *FEMA 427*, Washington, D.C.
- Gale, S., and Husick, L. (2003). *From MAD (mutual assured destruction) to MUD (multilateral unconstrained disruption): Dealing with the new terrorism*, Foreign Policy Research Institute, Washington, D.C.
- Garrett, L. (2000). *Betrayal of trust: The collapse of global public health*, Hyperion, New York.
- Gilbert, P., et al. (2003). "Infrastructure issues for cities—countering terrorist threat." *J. Infrastruct. Syst.*, 9(1), 44–54.
- Haimes, Y. Y. (2002). "Risk of terrorism to cyber-physical and organizational-societal infrastructures." *Public Works Manage. Policy*, 6(4), 231–240.
- Institute of Medicine (IOM). (2000). *To err is human: Building a safer health system*, National Academy Press, Washington, D.C.
- Kaplan, S., and Garrick, B. J. (1981). "On the quantitative assessment of risk." *Risk Anal.*, 1(1), 11–27.
- Kletz, T. (2001). *Learning from accidents*, Gulf Professional, Oxford, U.K.
- Kleindorfer, P. R., Kunreuther, H. C., and Schoemaker, P. J. (1993). *Decision sciences, An integrative perspective*, Cambridge University Press, New York.
- Klinenberg, E. (2002). *Heat wave: A social autopsy of disaster in Chicago*, University of Chicago, Chicago.
- Krugman, P. (2001). "Paying the price." *New York Times*, Sept. 16.
- Langewiesche, W. (2002). "American ground: Unbuilding the World Trade Center." *The Atlantic Monthly*, 290(2), 44–79.
- Linstone, H. (1984). *Multiple perspectives for decision making: Bridging the gap between analysis and action*, Elsevier, New York.
- Lipton, E., and Glanz, J. (2002). "9/11 prompts new caution in skyscraper design." *N.Y. Times*, Sep. 9.
- Little, R. G. (1999). "Educating the infrastructure professional: A new curriculum for a new discipline." *Public Works Manage. Policy*, 4(2), 93–99.
- Little, R. G. (2002a). "Controlling cascading failure: Understanding the vulnerabilities of interconnected infrastructures." *Journal of Urban Technology*, 9(1), 109–123.
- Little, R. G. (2002b). "A probabilistic approach for protecting people and buildings from terrorist attack and other hazards." *Proc., Int. Conf. on Protecting Structures Against Hazards*, C. I. Premiere, Singapore, 49–56.
- Marburger, J. (2002). *Testimony before the House Committee on Science*, June 14, 2002.
- Marshall, H. E. (2002). "Economic approaches to Homeland Security for constructed facilities." *Proc., 10th Joint W055-W065 Int. Symp. on Construction Innovation and Global Competitiveness*, Univ. of Cincinnati, Cincinnati.
- Mays, G. C., and Smith, P. D. (1995). *Blast effects on buildings*, Thomas Telford, London.
- Mileti, D. S. (1999). *Disaster by design: A reassessment of natural hazards in the United States*, Joseph Henry, Washington, D.C.
- Miller, J. (2003). "U.S. is deploying a monitor system for germ attacks." *N.Y. Times*, Jan. 22.
- Mlakar, P. F., Dusenberry, D., Harris, J. R., Haynes, G., Phan, L., and Sozen, M. (2003). *The Pentagon Building Performance Report*, ASCE, Reston, Va.
- Multidisciplinary Center for Earthquake Engineering Research (MCEER). (1995). "The Hanshin-Awaji earthquake of January 17, 1995: performance of lifelines." *Technical Rep. MCEER-95-0015*, Buffalo, N.Y.
- Multidisciplinary Center for Earthquake Engineering Research (MCEER). (2002). *Proc., Workshop on Lessons Learned from the World Trade Center Attack: Management of Complex Civil Emergencies and Terrorism-Resistant Civil Engineering Design*, Buffalo, N.Y.
- National Academy of Engineering (NAE). (1988). *Cities and their vital systems: infrastructure past, present, and future*, J. H. Ausubel, and R. Herman, eds., National Academy Press, Washington, D.C.
- National Institute of Standards and Technology (NIST). (1994). *1994 Northridge Earthquake: Performance of Structures, Lifelines, and Fire Protection Systems*, NIST, Gaithersburg, Md.
- National Research Council (NRC). (1985). *Safety of dams, flood and earthquake criteria*, National Academy Press, Washington, D.C.
- National Research Council (NRC). (1994). *Practical lessons from the Loma Prieta earthquake*, National Academy Press, Washington, D.C.
- National Research Council (NRC). (2000). *Blast mitigation for structures: 1999 status report on the DTRA/TSWG Program*, National Academy Press, Washington, D.C.
- National Research Council (NRC). (2002). *Making the nation safer: the role of science and technology in countering terrorism*, National Academy Press, Washington D.C.
- National Research Council (NRC). (2003). *Working in Olmsted's shadow: guidance for developing a scope of services for the update of the master plan for the U.S. Capitol and grounds*, National Academy Press, Washington, D.C.
- O'Rourke, T. D., Lembo, A. J., and Nozick, L. K. (2003). "Lessons learned from the World Trade Center disaster about critical utility systems." *Beyond September 11th: An Account of Post-Disaster Research*, M. F. Myers, ed., Natural Hazards Research and Applications Information Center, Univ. of Colorado, Boulder, Colo.
- Padfield, P. (1995). *War beneath the sea*, Wiley, New York.
- Petak, W. J. (2003). "Implementing earthquake mitigation: The context counts." *Proc., 55th Annual Meeting*, Earthquake Engineering Research Institute, El Oro, Calif.
- Perrow, C. (1999). *Normal accidents: Living with high-risk technologies*, Princeton University, Princeton, N.J.
- Petroski, H. (1992). *To engineer is human: The role of failure in successful design*, Vintage, New York.
- Petroski, H. (1994). *Design paradigms: Case histories of error and judgment in engineering*, Cambridge University, Cambridge, U.K.
- Rypkema, D. (2003). "The importance of downtown in the 21st century." *J. Am. Plan. Assn.*, 69(1), 9–15.
- Schneier, B. (2003). "Locks and full disclosure." *Crypto-Gram Newsletter*, (<http://www.counterpane.com/crypto-gram-0302.html>) (July 9, 2003).
- Sevin, E., and Little, R. G. (1998). "Mitigating terrorist hazards." *The Bridge*, 28(3), 3–8.
- Spencer, B. F., Jr. (2002). "Smart structures technology: opportunities and challenges." *Presentation to the National Research Council Committee to Develop a Long-term Research Agenda for the Network for Earthquake Engineering Simulation*, National Research Council, Washington, D.C.
- Starr, C. (2003). "The precautionary principle versus risk analysis." *Risk Anal.*, 23(1), 1–3.
- Tamaro, G. J. (2002). "World Trade Center 'bathtub': From genesis to Armageddon." *The Bridge*, 32(1), 11–17.
- Tierney, K. (2002). "Overview: Conceptualizing and measuring resilience for physical and organizational systems." *Proc., Workshop on Lessons Learned from the World Trade Center Attack: Management of Complex Civil Emergencies and Terrorism-Resistant Civil Engineering Design*, Multidisciplinary Center for Earthquake Engineering Research, Buffalo, N.Y., 61–63.

- Wallace, W. A., Mendonca, D. M., Lee, E. E., Mitchell, J. E., and Chow, J. H. (2003). "Managing disruptions to critical interdependent infrastructures in the context of the 2001 World Trade Center attack." *Beyond September 11th: Account of Postdisaster Research*, M. F. Myers, ed., Natural Hazards Research and Applications Information Center, Univ. of Colorado, Boulder, Colo.
- Wiener, J., and Rogers, M. (2002). "Comparing precaution in the U.S. and Europe." *J. Risk Res.*, 5(4), 317–349.
- Wulf, W., Haimes, Y., and Longstaff, T. (2003). "Strategic alternative responses to risk of terrorism." *Risk Anal.*, 23(3), 429–444.
- Zimmerman, R. (2002). "Enhancing resilience of integrated civil infrastructure systems." *Proc., Workshop on Lessons Learned from the World Trade Center Attack: Management of Complex Civil Emergencies and Terrorism-Resistant Civil Engineering Design*, Multidisciplinary Center for Earthquake Engineering Research, Buffalo, N.Y., 65–66.