The International Emergency Management Society
9th Annual Conference Proceedings
University of Waterloo, Canada, May 14-17, 2002

UNDERSTANDING AND CONTROLLING CASCADING FAILURE: A SYSTEMS APPROACH TO MULTI-HAZARD MITIGATION

Richard G. Little, AICP[1]

National Research Council

Keywords: hazard mitigation, infrastructure protection, building security, risk management

Abstract

Civil infrastructures (including buildings) are vital elements of a nation's economy and quality of life. They represent a massive capital investment, and, at the same time, are an economic engine of enormous power. Modern economies rely on the ability to move goods, people, and information safely and reliably. Consequently, it is of the utmost importance to government, business, and the public at-large that the flow of services provided by a nation's infrastructure continues unimpeded in the face of a broad range of natural and manmade hazards. The built environment must be designed to resist a formidable array of natural and man-made hazards over its lifetime. In the natural realm, earthquakes, extreme winds, floods, snow and ice, volcanic activity, landslides, tsunamis, and wildfires all pose some degree of risk to infrastructure systems. To this list of natural hazards, we must add terrorist acts, errors in design, construction, or operation, excessively prolonged service lives of materials and components, and inadequate maintenance. In a continuous search for increased efficiency, our way of life has become dependent on tightly coupled, highly sophisticated networks of transportation, electric power, and telecommunications systems from which essentially all redundancy has been removed. These systems become vulnerable to failure simply through their inherent complexity—and although failure may be predictable—its mode and mechanisms are not. The terrorist attacks of September 11 provided ample and horrific evidence of a previously unimaginable complex system failure. The seemingly unrelated issues of passenger throughput and airport security were critical in producing the most devastating structural failure in history. Therefore, from a comprehensive hazard mitigation standpoint, it is always necessary to look beyond the first-order effects of an event and instead seek to understand the perturbed behaviors of a complex, "system of systems". Making these systems inherently safer will require more than just improved engineering and technology. Complex systems also have a critical human component that needs to be integrated into design and operational procedures.

Introduction

Civil infrastructures (including buildings) are vital elements of a nation's economy and quality of life. They represent a massive capital investment, and, at the same time, are an economic engine of enormous power. Modern economies rely on the ability to move goods, people, and information safely and reliably. Consequently, it is of the utmost importance to government, business, and the

---

[1] Director, Board on Infrastructure and the Constructed Environment, National Research Council, 2101 Constitution Avenue, NW, Washington, DC.

public at-large that the flow of services provided by a nation's infrastructure continues unimpeded in the face of a broad range of natural and manmade hazards.

This linkage between systems and services is critical to any discussion of infrastructure. Although it may be the hardware (i.e., the highways, pipes, transmission lines, communication satellites, and network servers) that initially focuses discussions of infrastructure, it is actually the services that these systems provide that are of real value to the public (Little, 1999). Therefore, high among the concerns in protecting these systems from harm is ensuring the continuity (or at least the rapid restoration) of service.

Causes and Consequences of Infrastructure Failure

The built environment must be designed to resist a formidable array of natural and man-made hazards over its lifetime. In the natural realm, earthquakes, extreme winds, floods, snow and ice, volcanic activity, landslides, tsunamis, and wildfires all pose some degree of risk to infrastructure systems. To this list of natural hazards, we must add terrorist acts, errors in design, construction, or operation, excessively prolonged service lives of materials and components, and inadequate maintenance. Although our knowledge of how and why these systems fail has improved, and engineering approaches to design infrastructure systems to withstand natural hazards have been developed, crippling failures continue to occur (Mileti, 1999).

The consequences of infrastructure failure can range from the benign to the catastrophic. For example, whereas a power outage or water main break may be cause for only minor annoyance, a street closure due to the formation of a sinkhole may cause major disruption. If the same sinkhole were to cause simultaneous failures in the water and natural gas systems, and resultant fires could not be fought effectively due to inadequate water supply or pressure, possible loss of life and property damage could far exceed expectations from the initial cause. For example, the B-25 airplane that struck the Empire State Building in 1945 caused relatively minor structural damage and little loss of life and was the genesis of the design scenario of a Boeing 707 striking one of the World Trade Center towers (Robertson, 2002). However, the actual attacks on the World Trade Center on September 11 precipitated total structural failure and were truly cataclysmic in both the extent of the physical damage and the number of casualties.

Although hazard mitigation has moved beyond purely life safety issues, the protection of lifeline infrastructures has generally focused on first order effects—designing systems to resist the loads imparted by extreme natural events, and more recently, malevolent acts such as sabotage and terrorism. However, as these systems become increasingly complex and interdependent, hazard mitigation must also be concerned with secondary and tertiary effects.

Interdependent Infrastructures

Mitigating damage to infrastructure and ensuring continuity of service is complicated by the interdependent nature of these systems. For example, although the interdependence of many systems is straightforward (e.g., the role played by electric power in providing other services is obvious), the interdependencies of other systems are no less real if not as visible.

Interdependent effects occur when an infrastructure disruption spreads beyond itself to cause appreciable impact on other infrastructures, which in turn cause more effects on still other infrastructures. When an infrastructure system suffers an outage, it is often possible to estimate the impact of that outage on service delivery. These are the "directly dependent effects" of the outage. However, that outage may also diminish the ability of other infrastructures, through no malfunction of their own, to deliver the level of services that they normally provide. These indirect effects make up a first-order interdependent effect.

The impact of the outage may not stop at these first-order effects. They may go on to adversely affect still other critical infrastructure components, including even the infrastructure that was the original source of the problem, further aggravating the situation. These effects become second-order effects, which can propagate still further, causing yet another round of effects. How far these effects propagate, and how serious they become, depends on how tightly coupled the infrastructure components are, how potent the effects are, and whether or not countermeasures such as redundant capacity are in place. Either the outage effects will die out as they move further away from the base outage, limiting overall damage, or they will gather force in successively stronger waves of cascading effects until part or all of the infrastructure network breaks down. In the latter case, losing a key component creates a much broader failure that is out of proportion to the original failure. Infrastructure failures may be broadly described in three categories:

- Cascading failure – a disruption in one infrastructure causes a disruption in a second infrastructure
- Escalating failure – a disruption in one infrastructure exacerbates an independent disruption of a second infrastructure (e.g., the time for recovery or restoration of an infrastructure increases because another infrastructure is not available)
- Common cause failure – a disruption of two or more infrastructures at the same time because of a common cause (e.g., natural disaster, right-of-way corridor)

The interdependency problem is further compounded by the extensive linkage of physical infrastructure with information technology systems. Communication and information technologies are already affecting infrastructure system design, construction, maintenance, operations, and control and more change appears inevitable. Potential applications include coupled sensing, monitoring, and management systems, distributed and remote wireless control devices, Internet-based data systems, and multimedia information systems. Although the coupling of physical infrastructure with information technology promises improved reliability and efficiency at reduced cost, there is surprisingly little known about the behavior of these coupled systems and thus, their potential for cataclysmic failure is high.

Although long recognized as a serious concern, the issue of infrastructure interdependency has only recently begun to receive serious attention. The potential for failures in one infrastructure system to cause disruptions in others that could ultimately cascade to still other systems with unanticipated consequences is very real. In truth, beyond a certain rudimentary level, the linkages between infrastructures, their interdependencies, and possible failure mechanisms are not well understood.

Closely Coupled Complex Systems

In his book, *Normal Accidents* (Perrow, 1999a), Charles Perrow described numerous failures of tightly coupled, complex systems.[2] In our search for speed, volume, efficiency, and the ability to operate in hostile environments, he maintains that we have neglected the kind of system designs that provide reliability and security (Perrow, 1999b). A particularly troubling characteristic of these tightly-coupled, complex systems is that although failure is predictable the mode is not (in other words, they will predictably fail but in unpredictable ways). Similar chains of events do not always produce the same phenomena, but system level or "normal" accidents of major consequence continuously recur.

The catastrophic system failures that Perrow calls normal accidents cannot be dismissed as statistical anomalies—unique intersections of random events—but rather as the expected behavior

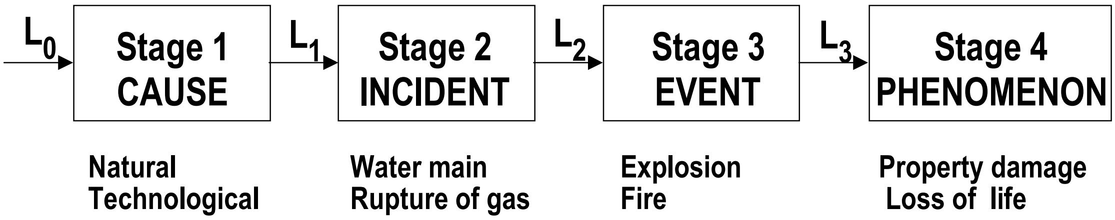
[2] These occur where the systems involved are sufficiently complex to allow unexpected interactions of failures to occur such that safety systems are defeated, and sufficiently tightly coupled to allow a cascade of increasingly serious failures ending in disaster.

of closely-coupled, complex systems. This supports a discomforting premise that although it may not be possible to predict the precise nature of the next Chernobyl, Bhopal, or major terrorist attack, a system failure of a similar cascading nature is destined to occur if we continue to rely on the types of critical-state systems underlying these disasters.

Understanding Interdependency

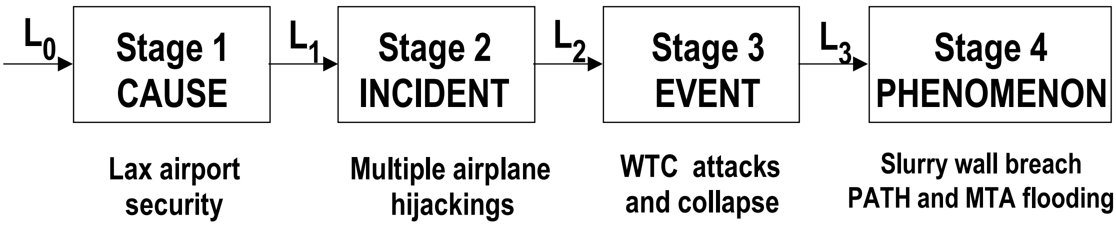
Baisuck and Wallace have developed a probabilistic model to analyze marine accidents (Baisuck and Wallace, 1979) and the multi-ordered implications of infrastructure failure can be generalized using a similar approach. As depicted in Figure 1, the first stage, or CAUSE, could be a natural hazard such as an earthquake or a technological hazard such as equipment or material failure. This is followed by the INCIDENT, in the examples above, the actual failure of the infrastructure with loss of water pressure and venting of natural gas. Stage 3, the EVENT, would be the resultant fires leading to Stage 4 PHENOMENON with property damage and loss of life.

Figure 1: A model for depicting the linked relationships between hazards and their ultimate outcomes (after Baisuck and Wallace, 1979).



Each stage in the process link is connected to the preceding and following stages by a probabilistic function based on the frequency of occurrence for any two linked stages. Thus, gas line ruptures in certain soil types (INCIDENT) can be linked to earthquakes of a certain magnitude (CAUSE) by obtaining the frequency with which gas line ruptures occurred as a result of an earthquake. If sufficient data exist, similar probabilistic analyses can be carried through the entire chain of events. A potential, but fortunately unrealized, outcome of the events of September 11 was the possible flooding and subsequent disruption of a large portion of New York's underground commuter rail system on which the City depends so heavily. Tamaro has described the damage to the slurry wall or "bathtub" that surrounded the deep basements of the World Trade Center and the extent of flooding (Tamaro, 2002). Had the slurry wall been extensively breached, it is possible that water from the Hudson River could have entered the MTA tunnels, flooded the system as far north as 34th Street, and subsequently spilled over to flood other parts of the system through their interconnected tunnels. Figure 2 is a useful logic model for depicting how a breakdown in one infrastructure system (passenger air travel) could have had unforeseen and devastating (but fortunately, unrealized) consequences for another (urban transit).

Figure 2: Logic model of an unrealized outcome of the events of September 11



The Human Element

Three Mile Island and Chernobyl provide useful case studies for understanding how systems might be designed to lessen the frequency and impact of cascading failures. In both cases, it was the intersection of concurrent failures in technology and human performance that was the key factor because neither failure alone would have produced the ultimate disastrous outcome (Perrow, 1999a; Chiles, 2001). Perrow believes that such failures are the inevitable consequence of closely-coupled complex systems and argues for what amount to safety valves and circuit breakers in terms of redundant technology and improved operator training and performance. At both Three Mile Island and Chernobyl, commonly held views of the situation were uniformly wrong and ultimately contributed to the system breakdowns. Fortunately, in the case of Three Mile Island, an outside agent who had not been influenced by observing the emerging events, was able intervene before total failure of the system (Chiles, 2001). None of the workers at Three Mile Island had been trained to expect anything resembling the types of problems that they actually had to confront. They had no successful patterns or strategies to call upon and were unable to adapt to the rapidly changing conditions.

Other Infrastructure Failures

Disastrous infrastructure failures with similar but subtler links between technology and human performance abound in the literature. The collapse of the Mianus River, Schoharie Creek, and Hatchie River Bridges and the Hyatt Regency Skywalk are illustrative in this regard. The Mianus River Bridge in the State of Connecticut carried Interstate 95. In 1983 a rusted hanger pin and hanger failed and caused a two-lane section of the roadway to fall into the river below resulting in the loss of three lives. Excessive rust had developed due to paved-over road drains and went unobserved because of poor inspection practices (NTSB, 1984). The Schoharie Creek Bridge, which carried the New York State Thruway, failed in 1987 after a pier was undercut by scour and fell into the creek. The bridge girders slipped off their supports and caused a section of the roadway to fall into the creek, killing ten people. Despite a report almost ten years earlier calling for replacement of missing riprap around the failed pier, the work was deleted from a maintenance contract (NTSB, 1988). In 1989, an 85-foot section of the bridge carrying U.S. Route 51 over the Hatchie River in Tennessee fell into the river after 2 columns supporting 3 bridge spans collapsed. Eight people were killed in an accident whose primary causes were a lack of redundancy in design and poor inspection and maintenance practices that failed to detect a developing problem (NTSB, 1990).

In 1981 a failure occurred that was described at that time as “the worst structural disaster in the United States” (Levy and Salvadori, 1992). The Skywalk at the Hyatt Regency Hotel in Kansas City, Missouri collapsed, killing 114 people and injuring more than 200. Through an unfortunate and bizarre sequence of events, a design that did not meet the applicable building code was produced by the structural engineer and was subsequently modified and *made weaker* by the contractor. The contractor’s shop drawings were later approved by the structural engineer and the effects of the change were never noticed (although it was never clear whether they were actually reviewed). The walkway was opened for use despite several instances during construction of the hotel when deficiencies were noted but were not acted upon (Petroski, 1992). Although not on the scale of a Three Mile Island or Chernobyl, what arguably places these four examples in the same context is the recurring intersection of technical faults and human performance failure. The critical role played by the human component of technological systems needs to be far better understood in the context of managing interdependent infrastructures in times of stress or crises.

Learning from Failure

Some form of structural failure analysis has probably existed since the time of Hammurabi if not before. Contract disputes over shoddy work or construction failures required that someone conduct an investigation and determine, as best they were able, the cause of failure and who was at fault. Forensic engineering is now a healthy, mature discipline and much knowledge has been gained, and advances made, from the study of engineering failures (Petroski, 1992, 1994). Engineering approaches to hazard-resistant design for structures and lifeline systems have improved continuously from the observation of past failures, assessment of their causes, and improvements in techniques and materials (Mileti, 1999; NRC, 1994). However, despite the value of forensic engineering to the advancement of engineering practice, the system is far from ideal. Much work of value exists only in court records, sealed by litigation settlements. Nothing analogous to the Air Safety Reporting System[3] exists for engineering practice although the Near-Miss Project at the Wharton School of the University of Pennsylvania is an attempt to develop a similar reporting framework for other industries (Phimister, et al., 2000). There are also conceptual concerns with commonly used forensic techniques. In its study of errors in the health care industry, *To Err Is Human*, the Institute of Medicine noted that:

> 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).

In light of this, care needs to be taken so that lessons learned programs (or other forms of adaptive learning for understanding the failure mechanisms of interdependent infrastructures) are designed to capture the influence of all contributing factors, not merely the obvious or easy.

Understanding Building Failure

At the conclusion of their 1992 book, *Why Buildings Fall Down*, Matthys Levy and Mario Salvadori posed the question of whether progress in the field of structures would reduce the number of failures (Levy and Salvadori, 1992). In light of the devastating collapse of the World Trade Center towers, this question is certainly as relevant today as when first posed a decade ago. However, a series of other structural failures through the 1990's raises the more compelling question of whether the overall state of knowledge regarding the interplay of risk factors in design and construction is adequate to ensure the integrity and safety of buildings and those who inhabit them. For example, the progressive collapse of the Alfred P. Murrah Federal Building in Oklahoma City in the aftermath of the 1995 bombing; extensive and costly damage to steel-frame buildings following the 1994 Northridge earthquake; damage to buildings due to snow loadings in Washington, Oregon and California caused by winter storms in 1996 are examples of failed designs employing what might be reasonably judged to be the best available practice or technology of the time. However, when subjected to extreme loading conditions, the designs proved inadequate.

---

[3] The ASRS is a voluntary program administered by NASA wherein air safety-related incidents and near accidents can be reported without fear of self-incrimination. The program is credited with facilitating beneficial change throughout the airline industry (Perrow, 1999).

As isolated events, these examples would traditionally warrant a comprehensive but narrowly focused forensic investigation of the failure modes, their likely causes, and possible remedial actions (Feld and Carper, 1997). However, when considered together, these and other structural failures worldwide suggest the need for a broader, systematic contemplation of structural design and the degree to which the ultimate safety of a building's occupants depends on design assumptions that may or may not be valid under extreme loading conditions. This was dramatically demonstrated by the World Trade Center and is particularly critical in light of continuing emphasis on taller and lighter buildings (often in areas of high seismic and extreme wind risk) and the desire to accelerate the deployment of new materials and technologies into building construction.

Progressive Collapse

Progressive structural collapse occurs when the loss of load-bearing capacity (for example, through the destruction of one or more columns, or of load-bearing walls) results in localized structural failure that leads to further loss of support and, ultimately, collapse of all or part of the structure. The extent of total damage is disproportionate to the original cause. Redundancy in the design can provide multiple load paths to the ground so that if one or more load-bearing elements are compromised, sufficient capacity remains to support the structure. Better continuity in structural joints between beams, columns, and floor slabs by means of increased reinforcement is one means of ensuring redundant load paths. Although there are ways to reduce the tendency of a building to undergo progressive collapse, there is no uniform, straightforward solution to this problem, because our current knowledge of the mechanisms of progressive collapse is incomplete. Following the collapse of the Ronan Point apartment building in Great Britain as the result of a gas explosion in 1968, there was considerable interest in progressive collapse. Although some advances were made in the 1970s, research funding waned in the absence of continuing public concern.

Progressive collapse is a principal, if not the leading, cause of injury and death in building failures, regardless of the source of the loading (e.g., bomb, earthquake, internal explosion) (NRC, 2000). For this reason, predicting and designing to prevent the progressive collapse of a building for various terrorist attack scenarios is a high priority for structural engineering research. Further increasing our understanding of progressive collapse will require both physical testing of structures at full and partial scales, coupled with advanced computer modeling. However, because buildings are complex systems that can have large variances between design specifications and as-built conditions, a test structure may not accurately mimic the progressive failure of a real building. Although an experienced engineer can often estimate the likelihood that a specific building will collapse by superimposing a damage scenario on the design, because of the variances described above, the actual progress of a collapse is essentially a chaotic process. For example, following major earthquakes, nonstructural building components, such as mechanical piping, partition walls, equipment, heavy-duty storage facilities (shelving and file cabinets), and curtain walls that can transfer some of the dead load to lower levels, have been observed to keep buildings standing that would otherwise have been expected to fail (NRC, 2000). This phenomenon, (i.e., a complete progressive failure that is just barely contained) has been observed in Mexico, California, Japan, Guam, and more recently in Turkey and Taiwan. Unfortunately, although nonstructural elements obviously have an important role to play in determining individual outcomes, their random contribution to preventing a collapse cannot be easily included in structural models.

Protecting People and Buildings from Terrorism

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 may be achieved through the integration of four fundamental security design objectives:

(1) denying the means of attack
(2) maintaining safe separation of attackers and targets through good planning and architectural practice
(3) providing strong, resilient construction to protect people and key building assets
(4) facilitating rescue and recovery operations in the event an attack occurs.

As demonstrated by the terrorist attacks of September 11, the first line of defense must be to identify and apprehend potential perpetrators before they can act. They must also be denied access to the means of attack such as explosives and delivery vehicles. This encompasses a broad range of primarily security-related activities such as domestic and international intelligence and surveillance, domestic law enforcement, enhanced airport security, and improved explosive-detection devices.

The second and third objectives require the active collaboration of engineers, architects, landscape architects, security specialists, and others to ensure the attractive integration of site and structure in a manner that minimizes the opportunity for attackers to approach or enter a building. They include such features as landscaping and earthworks that can function both as blast barriers and vehicle controls and appropriately designed street furniture such as planter boxes and bollards that prevent vehicular access. The building itself may have a range of blast-resistant features such as additional reinforcing details, composite fiber wraps to strengthen columns and slabs, and high-performance glazing materials. The structure's electrical and utility systems may be placed in protected raceways, critical facilities or operations housed in specially hardened areas or underground, and primary and backup systems located in different parts of the building.

As the tragic events of September 11 made abundantly clear, it is difficult if not impossible to prevent destructive acts by persons unconcerned with their own safety or survival. Therefore, facilitating rapid rescue and recovery of victims in the aftermath of an attack is a key component of a building protection strategy. The speed with which rescue personnel can safely enter and secure a damaged building can reduce the loss of life, mitigate injuries, prevent further damage to the structure, and help restore the building to productive use.

Assessing and Managing Infrastructure Risk

Risk gives meaning to things, forces, or circumstances that pose danger to people or what they value (NRC, 1996). Descriptions of risk are typically stated in terms of the likelihood of harm or loss from a hazard and usually include an identification of what is "at risk" and may be harmed or lost; the hazard that may occasion this loss; and a judgment about the likelihood that harm will occur. In the context of physical infrastructure, *risk* connotes the likelihood and level of failure of a critical physical or operational system that would prevent an infrastructure element from fulfilling its primary mission, i.e., providing services. To assess these risks, systemic quantitative risk assessment and management is necessary.

In the context of building security and hazard mitigation, *risk* connotes the likelihood and level of failure of a critical physical or operational system that would prevent the building from fulfilling its primary mission, i.e., protecting the people within. To assess these risks, systemic quantitative risk assessment and management is necessary.

In *risk assessment,* three questions must be answered (Kaplin and Garrick, 1981):

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

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, benefits, and risks*? (For example, increased cost would be traded off with reduced risk and improved confidence in the system.)
- *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.).

Any actions taken to develop and implement comprehensive hazard mitigation strategies for buildings and infrastructure must be based on a balanced assessment of all risks confronting the systems and the possible consequences of their failure, either singly or in combination with other, interconnected systems. These strategies must be informed by the best available information and carried out by people knowledgeable about the systems, their possible failure modes, the implications of concurrent system failures, and possible interventions that would allow systems to degrade gracefully and avoid catastrophic, multi-system failure.

Conclusions

Although recent events have focused on malevolent acts and how to prevent them, infrastructure faces other equally serious threats. In addition to natural hazards, the literature demonstrates that excessively prolonged service lives, aging materials, and inadequate maintenance all negatively affect infrastructure. Although, there is strong capability within the hazard community for identifying and assessing these vulnerabilities, without a better understanding of the overall context in which they need to be applied, vulnerability assessment represents only part of a total systems solution. Infrastructure and building protection is not seen as a purely developmental problem but one in which basic research is necessary and, to date, insufficient. Research needs run the gamut from a better understanding of networks and interconnections, to the mechanism and prevention of progressive collapse, to improved operational guidance for emergency responders.

A Closing Caution

In *Betrayal of Trust*, (Garrett, 2000), Laurie Garrett paints 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, under-funded, and under-appreciated appendage. Today's concerns with bio-terrorism have the public and policy makers alike wondering if the U.S. is capable of dealing with deliberately induced outbreaks of infectious disease. However, terrorism may not be the real threat. The global economy and worldwide air transportation network have created a closely-coupled system that make it possible, and even likely, that someone infected with a highly contagious disease unwittingly will spread the infection far beyond their borders. In the absence of a global public health infrastructure, the potential consequences are grim. As she points out:

> High-tech solutions, devices to "sniff out" nasty microbes in the air or detect them in the water supply are a technological solution to a public health threat. Were a biological attack to occur, or a naturally arising epidemic, the public would have only one viable direction in which to place its trust: with its local, national, and global public health infrastructure. If such an interlaced system did not exist at a time of grave need it would constitute an egregious betrayal of trust.

Hopefully, no bio-disasters or further acts of terrorism will come to pass. But those concerned with physical infrastructure should take careful note of the warning implied. Our basic systems are at risk from threats we may not yet foresee. We need to anticipate these threats to our physical infrastructures, design systems that are inherently safer and more robust, and be prepared to restore them when they fail. As Leslie Robertson has recently written about the failure of structures that he designed,

> Surely, we have all learned the most important lesson—that the sanctity of human life rises far above all other values (Robertson, 2002).

References

Baisuck, A. and Wallace, W.A. 1979. A Framework for Analyzing Marine Accidents. Marine Technology Society Journal. 13(5):8-14.

Chiles, J.R. 2001. Inviting Disaster: Lessons From The Edge of Technology. New York, N.Y.: HarperCollins Publishers.

Ellingwood, B. R. and Leyendecker, E. V. 1977. Design Methods for Reducing the Risk of Progressive Collapse in Buildings. Washington, D.C: National Bureau of Standards.

Feld, J. and Carper, K.L. 1997. Construction Failure, 2nd edition. New York, N.Y.: John Wiley & Sons.

Garrett, L. 2000. Betrayal of Trust: The Collapse of Global Public Health. New York, N.Y.: Hyperion Books.

Haimes, Y.Y. 2002. Risk of Terrorism to Cyber-physical and Organizational-societal Infrastructures. Public Works Management and Policy. 6(4):231-240.

IOM (Institute of Medicine). 2000. To Err Is Human: Building A Safer Health System. Washington, D.C.: National Academy Press.

Kaplan, S. and Garrick, B.J. 1981. On the Quantitative Assessment of Risk. Risk Analysis. 1(1):11-27.

Levy, M. and Salvadori, M. 1992. Why Buildings Fall Down. New York, N.Y.: W.W. Norton & Company.

Little, R. G. 1999. Educating the Infrastructure Professional: A New Curriculum for a New Discipline. Public Works Management and Policy. 4(2):93-99.

Mileti, D.S. 1999. Disaster by Design: A Reassessment of Natural Hazards in the United States. Washington, D.C.: Joseph Henry Press.

NRC (National Research Council). 1994. Practical Lessons From the Loma Prieta Earthquake. Washington, D.C.: National Academy Press.

NRC. 1996. Understanding Risk: Informing Decisions in a Democratic Society. Washington, D.C.: National Academy Press.

NRC. 2000. Blast Mitigation for Structures: 1999 Status Report on the DTRA/TSWG Program. Washington, D.C.: National Academy Press.

NTSB (National Transportation Safety Board). 1984. Collapse of a Suspended Span of Route 95 Highway Bridge over the Mianus River, Greenwich, Connecticut. HAR-84/03. Washington, D.C.: National Transportation Safety Board.

NTSB. 1988. Collapse of New York Thruway (I-90) Bridge, Schoharie Creek, near Amsterdam, New York. HAR-88/02. Washington, D.C.: National Transportation Safety Board.

NTSB. 1990. Collapse of the Northbound U.S. Route 51 Bridge Spans over the Hatchie River near Covington, Tennessee. HAR-90/01. Washington, D.C.: National Transportation Safety Board.

Perrow, C. 1999a. Normal Accidents: Living with High-Risk Technologies. Princeton, N.J.: Princeton University Press.

Perrow, C. 1999b. The Vulnerability of Complexity. Presented at the Planning Meeting on the Role of the National Academies in Reducing the Vulnerabilities of Critical Infrastructures held at the National Academy of Sciences, April 28-29, 1999. Washington, D.C.

Petroski, H. 1992. To Engineer Is Human: The Role of Failure in Successful Design. New York, N.Y.: Vintage Books.

Petroski, H. 1994. Design Paradigms: Case Histories of Error and Judgment in Engineering. Cambridge, U.K.: Cambridge University Press.

Phimister, J.R., Oktem, U., Kleindorfer, P.R., and Kunreuther, H. 2000. Near-Miss System Analysis: Phase I. Working Paper of the Near-Miss Project, Wharton School, Center for Risk Management and Decision Processes. Available on-line at: http://grace.wharton.upen.edu/risk/wp/wplist00.html.

Robertson, L.E. 2002. Reflections on the World Trade Center. The Bridge. 32(1):5-10.

Sevin, E. and Little, R.G. 1998. Mitigating Terrorist Hazards. The Bridge. 28(3):3-8.

Tamaro, G.J. 2002. World Trade Center "Bathtub": From Genesis to Armageddon. The Bridge. 32(1):11-17.

Author Biography

Richard G. Little is Director of the Board on Infrastructure and the Constructed Environment of the National Research Council (NRC) where he develops and directs a program of studies in building and infrastructure research and maintains outreach and liaison with federal agencies, the legislative branch, and affiliated organizations. He has directed NRC study activities, participated in workshops and panels, and written several papers dealing with blast-effects mitigation and critical infrastructure protection. Mr. Little has over thirty years experience in planning, management, and policy development relating to public facilities. He has been certified by examination by the American Institute of Certified Planners and is a member of the Federal Planning Division of the American Planning Association. Mr. Little holds a B.S. in Geology and an M.S. in Urban-Environmental Studies, both from Rensselaer Polytechnic Institute.