

# Toward More Robust Infrastructure: Observations on Improving the Resilience and Reliability of Critical Systems

Richard G. Little, AICP  
National Research Council  
[rlittle@nas.edu](mailto:rlittle@nas.edu)

## Abstract

*Civil infrastructure provides the range of essential services generally necessary to support a nation's economy and quality of life—arguably entire 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. From a comprehensive vulnerability assessment and hazard mitigation standpoint, it is necessary to look beyond the effects of an event on a single system and instead seek to understand the perturbed behaviors of a complex, "system of systems". Making our infrastructure systems inherently safer when stressed also will require more than just improved engineering and technology. The events of September 11 demonstrated that these complex systems also have critical institutional and human components that need to be understood and integrated into design and operational procedures.*

## 1. Introduction<sup>1</sup>

Civil infrastructures are vital public artifacts that support 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.

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 is of real value to the public [2]. Therefore, high among the concerns in protecting these systems from harm is ensuring the continuity (or at least the rapid restoration) of service. The importance of the services that these systems provide to overall national security was noted in the 1997 report of the President's Commission on Critical Infrastructure Protection (PCCIP) which proposed a national strategy for protecting and assuring the continuity of critical infrastructures from physical and cyber threats. For the purposes of the commission's work, critical infrastructures were defined as systems whose incapacity or destruction would have a debilitating impact on the defense or economic security of the nation. They include telecommunications, electrical power systems, gas and oil, banking and finance, transportation, water supply systems, and government and emergency services [3].

## 2. Causes and Consequences of Infrastructure Failure

Over their lifetime, physical infrastructure systems must resist a formidable array of threats and insults. In the natural realm, earthquakes, extreme winds, floods, snow and ice, volcanic activity, landslides, tsunamis, and wildfires all pose some degree of risk. To this list of natural hazards, must be added terrorist acts, design faults, excessively prolonged service lives, aging materials, and inadequate maintenance. Although analysis of past events, improved prediction and forecasting methods, and engineering approaches to design and construction have improved the ability of infrastructure systems to withstand natural hazards, crippling failures continue to occur [4].

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

---

<sup>1</sup> Many of the thoughts that form the basis for this paper were originally presented in [1].

only minor annoyance, a street closure due to the formation of a sinkhole may cause major disruption. If the same sinkhole were to cause breakage in water and natural gas piping, it is possible that any resultant fires could not be fought effectively due to inadequate water supply or pressure. The possible loss of life and property could far exceed expectations from the initial cause. Fires following earthquakes are obvious examples of how a single hazard event can have consequences far beyond the initial damage as demonstrated in San Francisco in 1906 and in Kobe, Japan in 1995. Hazard mitigation for such lifeline infrastructures as water, electricity, and communications has generally focused on first order effects—designing the 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 the secondary and tertiary failure effects of these systems on each other. Furthermore, and perhaps even more significant, are the impacts of complex infrastructure system failures on our social, economic, and political institutions.

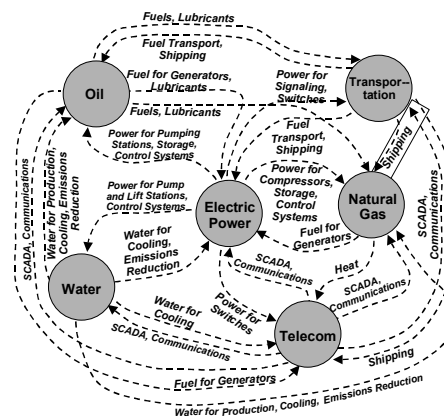
### 3. Interdependent Infrastructures

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. Figure 1 depicts some of the interconnections that exist between our basic service infrastructures.

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 disruption may not stop at these first-order effects. They may go on to adversely affect still other critical infrastructure components, possibly the system that was the original source of the problem further aggravating the situation. These second-order impacts 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 initiating cause, and whether or not countermeasures such as redundant capacity are in place. The outage effects will either die out as they move further away in time and space from the initiating event, limiting overall damage, or they will gather force in successively stronger cascading waves 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.



**Figure 1. Interdependencies between common infrastructure systems [5]**

Given the linkages among infrastructures, a cascading failure could well cross infrastructure boundaries, as demonstrated by the 1998 Galaxy IV satellite failure. When the PanAmSat Galaxy IV communication satellite rotated out of its orbital position in May, 1998, over 80 per cent of the digital pagers in the U.S. went off-line. Cable and broadcast transmissions were affected, as were credit card authorizations and ATM transactions. This event could have serious human impacts as many hospitals and healthcare providers in the United States faced a crisis in emergency communications when they could not page doctors and other care givers. This is particularly critical in a healthcare system which, in the quest for increased efficiency and productivity like much of the economy, relies on just-in-time service delivery. (The impacts of privatization, business reengineering, and process streamlining on infrastructure reliability and hence, service delivery, are discussed later in this paper.)

The Galaxy IV failure was not unique in either cause or consequence. Solar flares play havoc with satellite systems as do spikes in the Van Allen radiation belts. Since 1971, over 4500 incidents of satellite malfunction have been traced to the natural radiation environment. Other satellite failures have been ascribed to mechanical or other equipment breakdown. The interdependency problem is further compounded by the extensive

dependence of physical infrastructure with information technology systems. Communication and information technologies have had a significant impact on infrastructure system design, construction, maintenance, operations, and control and more change is 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. Software is fragile by nature and experience has shown that the software element of control and data acquisition systems is usually the least robust part of an integrated system.

Three broad classes of infrastructure failures can be described:

- 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)

Although recognized as a serious concern in certain industries, 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.

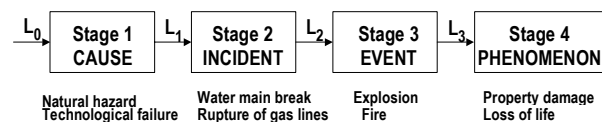
#### 4. Closely Coupled Complex Systems

In his book, *Normal Accidents*, Charles Perrow described numerous failures of what he describes as tightly coupled, complex systems (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.) [6]. In the 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 inherently provide reliability and security [7]. A particularly troubling characteristic of these tightly-coupled, complex systems is that they 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.

### 5. Understanding Interdependency

As a first approach, the multi-ordered implications of infrastructure failure can be generalized using a probabilistic model similar to that developed by Baisuck and Wallace to analyze marine accidents [8]. As depicted in Figure 1, the first stage (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 example of the sinkhole described earlier, the actual failure of the infrastructure with loss of water pressure and venting of natural gas. Stage 3 (EVENT), would be the fires resulting in Stage 4, property damage and loss of life.



**Figure 2. A model for depicting the linked relationships between hazards and their ultimate outcomes [8].**

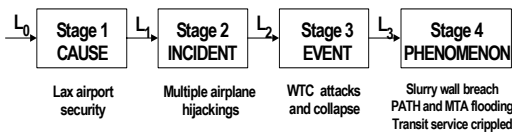
Each stage in the process link is connected to the preceding and following stages by a probabilistic function based on the frequency of occurrence for any two linked stages. Thus, gas line ruptures in certain soil types (INCIDENT) can be linked to earthquakes of a certain magnitude (CAUSE) by obtaining 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. Although this type of model can be useful for predicting outcomes when there is much historical data or when frequency relationships can be developed by other means, it is of lesser value when attempting to understand the extreme events that occur with limited frequency and are represented by the tails of probability functions.

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 rail transit 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 [9]. Langewiesche provides a chilling description of its possible failure:

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 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 [10].

Figure 3 depicts how a breakdown in one infrastructure system (passenger air travel) could have had unforeseen and devastating consequences for another (urban transit).



**Figure 3. Logic model of an unrealized outcome of the events of September 11**

## 6. Self-organized Criticality

Bak proposed the concept of self-organized criticality to explain how large dynamic systems can self-organize into a highly interactive critical state where even minor perturbations can lead to events, or “avalanches” of all sizes [11]. Self-organized criticality is probably a more powerful tool than a probability model for the study of cascading infrastructure failures because the tails of the frequency distributions of many extreme events behave in accordance with power laws that relate the number of events of different sizes by a constant proportion. Earthquakes are well suited to application of the principles of self-ordered criticality because according to Bak, “...large catastrophic events occur as a consequence of the same dynamics that produce small, ordinary events.” In other words, very large earthquakes appear to be generated by the same mechanisms as the many smaller events that never become very large. On this basis, the catastrophic system failures that Perrow calls normal accidents cannot be dismissed as statistical anomalies—unique intersections of very rare and random events—but rather as the expected behavior of, complex, self-ordering, and closely-coupled systems. Taken together, the work of Perrow and Bak supports a

discomforting premise that although it may not be possible to predict the precise nature of the next Chernobyl or Bhopal, a cascading failure of similar consequence is to be expected if we continue to rely on the types of critical-state systems that seem to be the root cause of these disasters.

## 7. Complex Adaptive Systems

Understanding how complex, interconnected infrastructure systems behave when subjected to the external stresses of natural and technological hazards presents enormous challenges. Managing such systems under these circumstances is even more difficult. Amin has described some of the challenges of avoiding failures in our complex national infrastructures [12]. These systems operate at the edge of stability, where the environment is constantly changing, and the systems must continuously adapt to the situation and each other. Complex Adaptive System (CAS) models may provide a framework for understanding and acting on events that occur in these chaotic circumstances. Axelrod and Cohen have used CAS models to describe the behavior of agents in biological and social systems as they learn, adapt, and evolve [13]. Their premise is that at the edge of chaos, which is disordered and unmanageable, complex systems exist. Although the behavior of these systems is hard to predict because of the many interacting agents, they behave according to some relatively simple rules and therefore can be understood, improved, and exploited.

Complex Adaptive Systems have many participants—often many kinds of participants—who interact in complicated ways that continuously reshape the future and generate new outcomes. Three key processes that are relevant to this discussion are Variation, Interaction, and Selection. Variation in an interactive system, as in a biological community, reduces the vulnerability to single point failures. The reduced efficiency brought about by independent elements (or evolutionary paths) is balanced by increased robustness of the system. By studying how interactive communities adapt, thrive, or perish, there is much to learn regarding what types of systems are inherently safer in practice. Similarly, interactions between members of the same group or social framework, while enhancing communication and simplifying information transfer, can have disastrous consequences when the jointly held information is wrong. Finally, selection deals with choosing successful strategies and rejecting those that lead to failure. The key here is learned behavior that will enable participants to survive in a complex, evolving environment. In the absence of actual conditions in which to learn adaptive behavior (such as warfare for the military) there is a need to train the participants by other means, e.g., gaming or simulation.

Three Mile Island and Chernobyl provide useful case studies for how CAS models can provide valuable insights 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 reinforcing failures in technology and human performance that led to disaster; neither the technological failures (which were relatively straightforward) or the operator errors alone would have produced the ultimate outcomes [6,14]. At both Three Mile Island and Chernobyl, the operators 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 to intervene before total failure of the system [14]. 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.

## 8. Other Infrastructure Failures

Disastrous infrastructure failures with similar but subtler links between technology and human performance abound in the literature. The collapse of several bridges in the United States in the 1980's (Mianus River, Schoharie Creek, and Hatchie River) and the Hyatt Regency Skywalk in Kansas City 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 [15]. 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 [16] and the bridge foundations were not regularly inspected. 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 [17].

In 1981 a failure occurred that was described at that time as "the worst structural disaster in the United States" [18]. 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 and which was essentially unbuildable was produced by the structural engineer. In an effort to ease constructability, the design 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 [19]. 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 complex infrastructure systems in times of stress or crises.

## 9. 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 [19,20]. 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 [4,21]. 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 (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 [6].) 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 [22].

However, there are 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. [23].

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.

## 10. Lessons Learned: September 11, 2001

Many years of observation of natural disaster events have produced a general postulate that *resilient* communities or systems (i.e., those having in place *robust* systems and institutions that possess a good deal of *redundancy*) fare the best [24]. This has recently been restated by Tierney in her assessment of New York City in the post-September 11 period [25]. For the sake of clarity, these terms are defined here [26].

**resilience** – the capability of a strained body to recover its size and shape after deformation; an ability to recover from or adjust easily to misfortune or change

**robust** – having or exhibiting strength or vigorous health; strongly formed or constructed

**redundant** – exceeding what is necessary or normal; serving as a duplicate for preventing failure of an entire system upon failure of a single component

Infrastructure systems in major urban areas are inherently interconnected and vulnerable to complex system failures. The attacks of September 11, 2001 provide some interesting lessons for understanding how the simple and straightforward concept of robustness and resilience played such a key role in the relatively rapid recovery of the city's infrastructures during of period of great stress and challenge. There have been several reconnaissance-level studies of the performance of infrastructure in the vicinity of the World Trade Center in the days and weeks following September 11 [25,27,28]. This work all underscores the notion that critical features of survivable systems are robustness, redundancy, and resilience and that it matters as much for institutions as it does for physical infrastructure and buildings. New York City was able to recover relatively quickly (compared to

how other cities might have fared) after September 11 because of the inherent redundancy of many of its physical and institutional infrastructures. Many of the service providers in New York (e.g., Consolidated Edison, Verizon, MTA) still possess considerable excess capacity in people, equipment, and other resources necessary to effect recovery. Leaner, less robust systems would probably not have performed as well and recovery would have been hampered.

Technology (e.g., sensors, communications, IT) was helpful in managing clean-up and recovery but more real-time capability is required. First responders in particular are in need of real-time data from damaged buildings coupled with assessment tools and decision-support systems so that the site commander can make informed choices about the feasibility of rescue operations versus the safety of emergency personnel. There are definitely opportunities to couple technologies in a manner that would enhance the safety and survivability of first responders.

## 11. Opportunities for Collaboration

While considering how complex infrastructures could be made more robust and resilient, several issues emerged in this paper that suggest collaboration between the social and physical sciences and engineering. Some approaches may be straightforward and call for the reinstatement of “shock absorbers and circuit breakers” in both a physical and operational sense to increase the resilience and reliability of infrastructure systems. Others will be more esoteric and call for the application of sophisticated analytical, modeling, and forecasting tools to improve understanding of the systems and the modes and consequences of failure. Still others may focus on the conflicts inherent in increased economic efficiency through capacity shedding, outsourcing, and just-in-time operational systems versus resilience-through-redundancy. There are many potential topics for research and they include such areas as:

- *Theoretical Foundations.* Research into the complex and adaptive behaviors of U.S. infrastructures and the overall behavior and functioning of the U.S. economy from an interdependent perspective is key if we are to understand how infrastructures will behave in the face of failure from a variety of causes—from physical or cyber attack, to a major earthquake, to failure of the network or its components.
- *Modeling and Simulation.* Modeling and simulation of interconnected complex infrastructures is rudimentary today. More advanced models, using actual regional or national infrastructure data, network layouts, and operating conditions are needed to uncover critical nodes, behaviors, and vulnerabilities.

- *Mitigation, Response, and Recovery.* In the event of a major infrastructure failure, isolating the affected portions of the system and preventing cascading failure will be important. Any mitigation actions will require accurate accounting of linkages among the infrastructures and the behaviors arising from such interdependencies. Appropriate and safe steps must also be identified for bringing the systems back on line.
- *Policy Research.* Policies affecting one infrastructure may have unintended consequences in others, due to the linkages involved. Little is known of how this happens and how to reduce the likelihood of its occurring. Likewise, in some cases appropriate policy decisions can probably forestall the need to make costly infrastructure expenditures.
- *The Human/Technological Interface.* Human error has played a major role in some of the most significant technological disasters of the past century. A better understanding of how systems can be designed to take human factors into account, as well as decision tools that enable people to structure rational choices for technological interaction, is needed.

## 12. Conclusions

Although recent events have focused on the impacts of 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. Despite this formidable array of threats confronting our infrastructures, many problems will occur simply due to the complexity of these systems. Potential failure nodes are repeatedly created at the intersections of tightly coupled, highly sophisticated transportation, electric power, and telecommunications systems and are compounded by their reliance on information systems and software. As a first step in protecting these systems, the "vulnerability of complexity" must be resolved.

Beyond generic complexity issues, there are specific emerging threats that are not well understood. For example, commercial satellites are playing an increasingly important role in earth observation, communication, and geospatial positioning—activities that are central to the control of many key civilian and military systems. This orbital infrastructure is vulnerable to natural events such as solar flares and radiation spikes as well as manmade threats such as electromagnetic pulse. Its ground-based elements are vulnerable to physical threats and terrestrial natural hazards. The vulnerability these satellites to ionizing radiation is of considerable concern to the defense establishment. These satellites

comprise the "eyes and ears" of the U.S. military and there is real concern that a hostile nation or non-state terrorist group could detonate a low-yield nuclear weapon in the Van Allen belts which could effectively negate much of the U.S.' technological superiority [29]. This situation could not be remedied by launching replacement satellites because the effects of the initial blast would linger for months to years.

Although, there is strong capability within the hazard community for identifying and assessing 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. Increasing the resilience and reliability of critical infrastructure is not 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 impacts of deregulation, privatization, and globalization, to better software and system designs. For example, an electric utility executive made the point in 1999 that she felt that the greatest threat to reliable service delivery was the local deregulation and decoupling of the industry that would enable the subsequent divestiture of less profitable elements of the electric power grid [30]. Amin has described an attempt to simulate how the emerging electric power industry might perform in these conditions through the use of a CAS model [31]. Although these are primarily institutional issues, they will have enormous impact on the reliability of the physical systems.

In an editorial for the *New York Times* entitled "Paying the Price" written shortly after the terrorist attacks of September 11, 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 [32]. He ascribes this largely to a national culture that is unwilling to pay the price of public safety and which depends on private companies to do a job that properly belongs in the public domain. He draws a parallel to the decay of the public health infrastructure in the United States that has been described by Garrett [33] and concludes with the notion that "...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."

## 13. A Closing Caution

In *Betrayal of Trust*, [33], Laurie Garrett paints a grim picture of how in the 20<sup>th</sup> 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 citizens and policy makers alike wondering if the U.S. is capable of dealing with deliberately induced outbreaks of

infectious disease (The very public national fumbling following the postal-based anthrax attacks in October, 2001 suggests that we are not [34]). 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 Garrett 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 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. In this regard, we should take counsel from this historical anecdote:

In 1346 a particular set of circumstances occurred, in a particular sequence, resulting in what may have been the first truly global epidemic. Perhaps only the Americas and Antarctica were spared humanity’s globalized Black Death. With epidemics, timing is everything [33].

## 14. References

[1] R.G. Little, “Controlling Cascading Failure: Understanding the Vulnerabilities of Interconnected Infrastructures”, *Journal of Urban Technology*, Carrfax Publishing,, pp.109-123, 2002.

[2] R.G. Little, “Educating the Infrastructure Professional: A New Curriculum for a New Discipline”, *Public Works Management and Policy*, pp. 93-99, 1999.

[3] The President’s Commission on Critical Infrastructure Protection (PCCIP). *Critical Foundations: Protecting America’s Infrastructures*. PCCIP, Washington, D.C., 1997.

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

[5] J. Peerenboom, R. Fisher, and R. Whitfield, 2001. “Recovering from Disruptions of Interdependent Critical Infrastructures” *Presentation to the workshop on Mitigating the*

*Vulnerability of Critical Infrastructure to Catastrophic Failures, September 10-11, 2001*. World Institute on Disaster Risk Management, Alexandria, Va., 2001.

[6] Perrow, C., *Normal Accidents: Living with High-Risk Technologies* Princeton University Press, Princeton, N.J., 1999.

[7] C. Perrow, “The Vulnerability of Complexity”, Paper presented at the *Planning Meeting on the Role of the National Academies in Reducing the Vulnerabilities of Critical Infrastructures, April 28-29, 1999*, National Academy of Sciences, Washington, D.C., 1999.

[8] Baisuck, A. and Wallace, W.A.. “A Framework for Analyzing Marine Accidents”, *Marine Technology Society Journal*, pp. 8-14, 1979.

[9] Tamaro, G.J. “World Trade Center “Bathtub”: From Genesis to Armageddon”, *The Bridge*, National Academy Press, Washington, D.C., pp. 11-17, 2002.

[10] Langewiesche, W. “American Ground: Unbuilding the World Trade Center”, *The Atlantic Monthly*, pp.44-79, 2002.

[11] Bak, P. and M. Paczuski, “Complexity, contingency, and criticality”, *Proceedings of the National Academy of Sciences*, National Academy Press, Washington, D.C., pp. 6689-6696, 1995.

[12] M. Amin, “National Infrastructures as Complex Interactive Networks”, in *Automation, Control and Complexity: An Integrated Approach*. Samad and Weyrauch, eds. John Wiley and Sons. New York, N.Y., 2000, pp. 263-286.

[13] Axelrod, R. and Cohen, M.D., *Harnessing Complexity: Organizational Implications of a Scientific Frontier*, Basic Books, New York, N.Y., 2000.

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

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

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

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

[18] Levy, M. and Salvadori, M. *Why Buildings Fall Down*, W.W. Norton & Compan, New York, N.Y., 1992.

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

- [20] Petroski, H., *Design Paradigms: Case Histories of Error and Judgment in Engineering*, Cambridge University Press, Cambridge, U.K., 1994.
- [21] NRC (National Research Council), *Practical Lessons From the Loma Prieta Earthquake*, National Academy Press, Washington, D.C., 1994.
- [22] Phimister, J.R., U. Oktem, P.R. Kleindorfer, and H. Kunreuther, "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://www.opim.wharton.upenn.edu/risk/proj/nearmiss.html>, 2000.
- [23] IOM (Institute of Medicine). *To Err Is Human: Building A Safer Health System*, National Academy Press, Washington, D.C., 2000.
- [24] Delmuth, J., *Countering Terrorism: Lessons Learned From Natural And Technological Disasters*, National Academy Press, Washington, D.C., 2002.
- [25] Tierney, K. "Overview of the Political, Economic, and Engineering Fusion of Resilience-enhancing Design", *Presentation to the Workshop on Lessons Learned from the World Trade Center Attack: Management of Complex Civil Emergencies and Terrorism-Resistant Civil Engineering Design, June 24-25, 2002. New York, N.Y.*, Multidisciplinary Center for Earthquake Engineering Research, 2002.
- [26] Webster, *Webster's Ninth New Collegiate Dictionary*, Merriam-Webster, Inc., Springfield, Mass., 1991.
- [27] Wallace, W.A. "How to Plan for Anything but a Repeat of the Past", *Presentation to the Workshop on Lessons Learned from the World Trade Center Attack: Management of Complex Civil Emergencies and Terrorism-Resistant Civil Engineering Design, June 24-25, 2002. New York, N.Y.*, Multidisciplinary Center for Earthquake Engineering Research, 2002.
- [28] Zimmerman, R. "Enhancing Resilience of Integrated Civil Infrastructure Systems", *Presentation to the Workshop on Lessons Learned from the World Trade Center Attack: Management of Complex Civil Emergencies and Terrorism-Resistant Civil Engineering Design, June 24-25, 2002. New York, N.Y.*: Multidisciplinary. Center for Earthquake Engineering Research, 2002.
- [29] Ullrich, G., *Presentation to the Planning Meeting on the Role of the National Academies in Reducing the Vulnerabilities of Critical Infrastructures, April 28-29, 1999*. National Academy of Sciences, Washington, D.C., 1999.
- [30] Wong, N., *Presentation to the Planning Meeting on the Role of the National Academies in Reducing the Vulnerabilities of Critical Infrastructures, April 28-29, 1999*, National Academy of Sciences, Washington, D.C., 1999.
- [31] M. Amin, "Restructuring the Electric Enterprise: Simulating the Evolution of the Electric Power Industry with Intelligent Adaptive Agents", in *Market Analysis and Resource Management*. Faruqui and Eakin, eds., Kluwer Publishers, Dordrecht, The Netherlands, 2002.
- [32] Krugman, P.. "Paying the Price", *New York Times*, September 16, 2001.
- [33] Garrett, L., *Betrayal of Trust: The Collapse of Global Public Health*, Hyperion Books, New York, N.Y., 2000.
- [34] A. Macintyre, "Chemical and Biological Weapons - Existing and Emerging Threats", *Presentation to the Seminar On Chemical And Biological Threats To Buildings, December 20, 2001*. Federal Facilities Council, Washington, D.C., 2001.