

28 October 2002



ROYAL  
ACADEMY  
of  
ENGINEERING

# The 3Rs: Lessons learned from September 11th

Robert Prieto

Chairman, Parsons Brinckerhoff Inc.

Co-chair, New York City Partnership Infrastructure Task Force



Sponsored by





**Robert Prieto**

As chairman of Parsons Brinckerhoff Inc., Bob Prieto heads PB's board of directors by overseeing management performance, establishing top-level policies, and ensuring the firm's continued long-term success after nearly 120 years of operation. As director of corporate development, a role he also fills, Mr Prieto oversees the continually expanding marketing and planning needs of a global company with more than 9,200 employees working from more than 200 corporate and project offices on six continents. In this capacity, he is responsible for strategic planning; management of the firm's marketing, sales and corporate communications efforts; and coordination and oversight of all marketing and sales operations, including government affairs activities, mergers and acquisitions, and activities of the business services group, which provides direct support to the firm's marketing and sales professionals across the world. He acts as treasurer of PB's political action committee, and has also served as corporate sponsor or principal-in-charge of several multibillion-dollar programs.

Mr Prieto served as co-chair of an infrastructure task force established by New York City Partnership and Chamber of Commerce that provided some of the earliest recommendations for transportation improvements in the aftermath of the September 11<sup>th</sup> attack. He is a member of the executive committee of the National Center for Asia-Pacific Economic Cooperation, member of the board of directors of the Business Council on International Understanding, chairman of the Engineering and Construction Governors of The World Economic Forum, and member of the Asia Society and several other national and international organizations. He is also a member of the board of trustees of Polytechnic University of New York, and was recently selected as alumni of the year by its New York Chapter. Mr Prieto holds an M.S. in nuclear engineering from Polytechnic University of New York and a B.S. in nuclear engineering from New York University.

**The 3Rs: Lessons learned from September 11<sup>th</sup>**

© Robert Prieto

*ISBN 1-903496-07-1*

*October 2002*

*Published by*

THE ROYAL ACADEMY OF ENGINEERING

29 Great Peter Street, Westminster, London SW1P 3LW

*Telephone 020 7222 2688 Facsimile 020 7233 0054*

[www.raeng.org.uk](http://www.raeng.org.uk)

*The Royal Academy of Engineering is a Registered Charity (No. 293074)*

# The 3Rs: Lessons learned from September 11<sup>th</sup>

A year has passed since the terrorist attacks on New York City and Washington, DC. For many, the memories, the sights and the sounds of that beautiful late summer day turned horrific will never be forgotten. Thousands died that day and the lives of millions of others were directly affected. In this lecture I try to provide a look back at September 11<sup>th</sup>, briefly recount the events of that day and the immediate aftermath, frame a set of lessons learned relevant to those responsible for infrastructure implementation, and briefly summarize where the rebuilding effort stands.

We cannot bring those that died that day back to life. Nor can we stop all deliberate acts of destruction targeted to our cities and their infrastructure. But we can improve the ability of our built environment to Resist, Respond and Recover from uncontrollable forces of nature and man. If this lecture helps ensure that neither the events of September 11<sup>th</sup> nor the lessons we should draw from it are forgotten, then it will be judged worthwhile. If not, history will write a different epitaph.

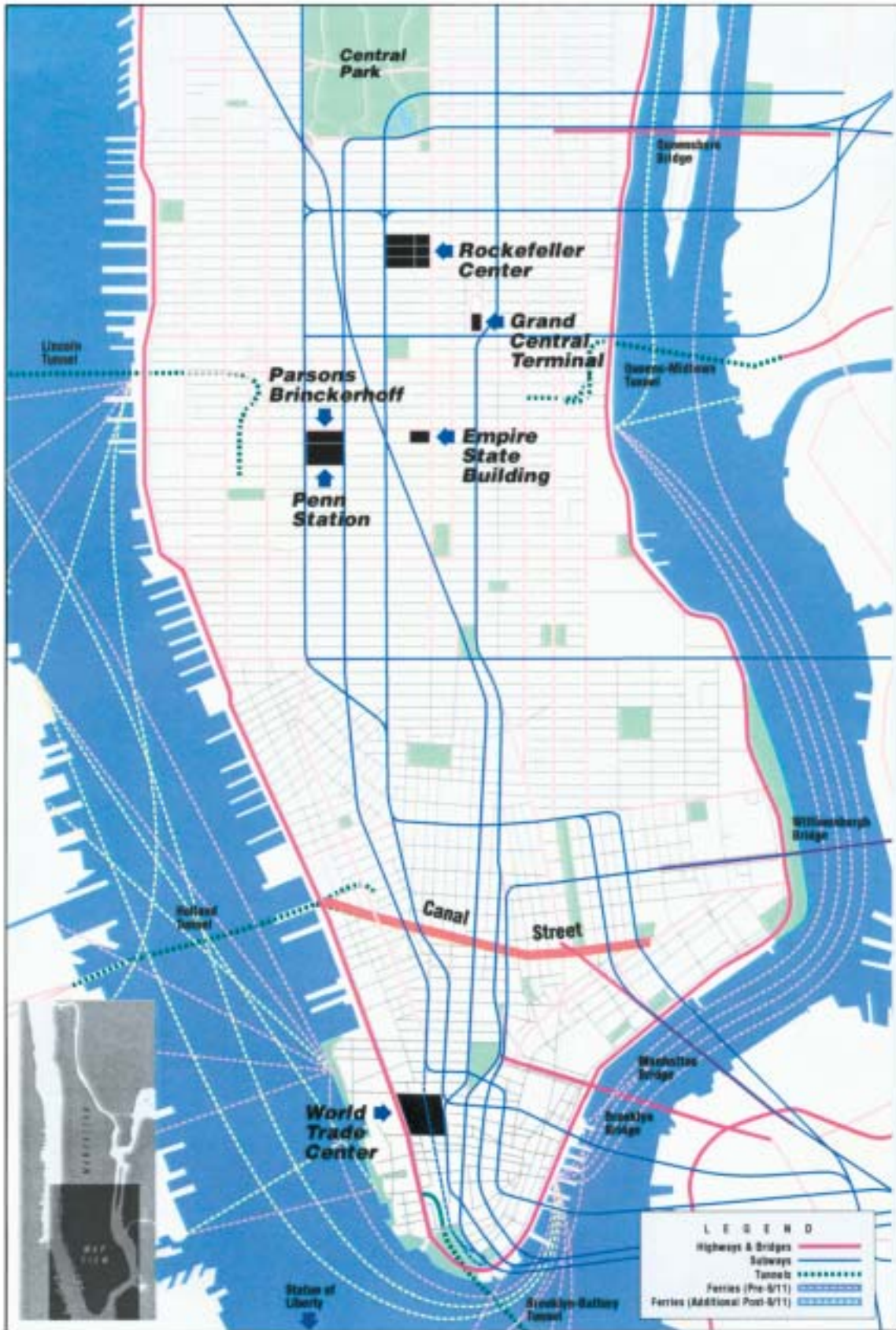
## **A Unique Perspective**

The thoughts that follow draw on my observations as a New Yorker, one who grew up and worked in the city throughout his entire career; as chairman of Parsons Brinckerhoff, New York's oldest engineering firm whose roots, reaching back to 1885, predate our work on New York City's first subway; and as co-chair of the Infrastructure Task Force established by the New York City Partnership in the aftermath of the attacks.

In essence, I believe history has handed our profession an unusual challenge as well as an unmatched opportunity. How we respond will say much about the future of the heavily engineered environment we call our cities as well as much about our own profession.

## **Events and Immediate Aftermath**

To fully appreciate the events that day, one must understand their rapidity and scale. Table 1 provides a more complete chronology, but within 18 minutes planes struck each of the two World Trade Center towers in New York. Eighteen minutes after the second plane struck the south tower, all bridges and tunnels into the New York City area were closed. Sixty-two minutes after the south tower was struck by United Airlines flight 175, it collapsed killing those still trapped inside as well as first responders who arrived to deal with the impact of American Airlines flight 11 into the north tower. The Port Authority Trans Hudson (PATH) line station was partially crushed by the collapse of the south tower. Twenty-three minutes later, the north tower collapsed.



*Table 1*  
**Chronology of September 11th**

<b>8:46 a.m.</b>	(all times are EDT): A hijacked passenger jet, American Airlines Flight 11 out of Boston, Massachusetts, crashes into the north tower of the World Trade Center, tearing a gaping hole and setting the building afire.
<b>9:03 a.m.</b>	A second hijacked airliner, United Airlines Flight 175 from Boston, crashes into the south tower of the World Trade Center and explodes.
<b>9:17 a.m.</b>	The Federal Aviation Administration shuts down all New York City area airports.
<b>9:21 a.m.</b>	The Port Authority of New York and New Jersey orders all bridges and tunnels in the New York area closed.
<b>9:40 a.m.</b>	The FAA halts all flight operations at U.S. airports, the first time in U.S. history that air traffic nationwide has been halted.
<b>9:43 a.m.</b>	American Airlines Flight 77 crashes into the Pentagon.
<b>10:05 a.m.</b>	The south tower of the World Trade Center collapses, plummeting into the streets below. A massive cloud of dust and debris forms and slowly drifts away from the building.
<b>10:10 a.m.</b>	A portion of the Pentagon collapses. United Airlines Flight 93, also hijacked, crashes in Somerset County, Pennsylvania, southeast of Pittsburgh.
<b>10:24 a.m.</b>	The FAA reports all inbound transatlantic aircraft flying into the U.S. are being diverted to Canada.
<b>10:28 a.m.</b>	The World Trade Center's north tower collapses from the top down as if it were being peeled apart, releasing a tremendous cloud of debris and smoke.
<b>11:02 a.m.</b>	New York City Mayor Rudolph Giuliani urges New Yorkers to stay at home and orders an evacuation of the area south of Canal Street.
<b>2:49 p.m.</b>	Subway and bus service is partially restored in New York City.
<b>4:10 p.m.</b>	Building 7 of the World Trade Center complex is reported on fire.
<b>5:20 p.m.</b>	The 47-story Building 7 of the World Trade Center complex collapses. The evacuated building is damaged when the twin towers across the street collapsed earlier in the day. Other nearby buildings in the area remain ablaze.



© 2001 AP

The collapse of the twin towers caused collateral damage of varying degrees to 29 million square feet of office space in lower Manhattan; started fires in nearby structures; and simultaneously caused major portions of the transportation, power, telecommunications and other infrastructure to be stressed to failure. Many of the lessons learned came from observing the relative response of these systems to the same originating event and failure environment.

A little over two hours after the first plane struck, an evacuation of southern Manhattan was ordered. Over the next several weeks, rescue efforts continued and critical infrastructure systems were restored pending permanent solutions.

The impacts are overwhelming:

- 2,801 people killed in New York
- 29,000,000 ft<sup>2</sup> damaged or destroyed
- New York City Emergency Operations Center destroyed
- 125,000 workers displaced
- Section of New York City subway destroyed by beams from the WTC
- PATH WTC station partially collapsed knocking one of three Hudson River crossings out of service
- 350,000 passengers initially displaced
- \$1.9 billion in telecom infrastructure destroyed
- Cell traffic to 10 cell sites knocked out
- Power grid lost two substations and local distribution system badly damaged
- Local power grid badly damaged
- Service disrupted to 12,000 electric customers; 270 steam customers; 1,400 gas customers.



© 2001 JOHN ALBANESE



### The 3Rs of Critical Infrastructure

What are we to learn as engineers from the attacks of September 11<sup>th</sup> and beyond? What are we to teach to those who follow in our footsteps? How are we to define “critical infrastructure” in the future?

These are but a few of the questions we must answer if we are to meet history’s challenge.

This need to learn...and to teach...has caused me to return to the age old fundamentals of education, namely the 3Rs. But in the 21<sup>st</sup> century’s highly engineered environment and with our increased recognition of the threats this environment faces, the traditional 3Rs of reading, ‘riting and ‘rithmetic have been replaced by Resist, Respond and Recover, at least as they relate to critical infrastructure.

In Table 2, I’ve provided a definition of critical infrastructure that builds upon and helps shape these 3Rs. It is important for us to recognize that each element of infrastructure is not of the same critical importance. We must focus our efforts to ensure that limited resources are most appropriately applied.

*Table 2*  
**Critical Infrastructure Defined**

- Systems whose *rapid* failure would lead to a catastrophic loss of life.
  - Systems whose failure or significant degradation would lead to unacceptable economic consequences.
  - Systems whose *rapid* failure would significantly impact rescue and response efforts.
  - Systems whose significant degradation significantly impact recovery efforts.
- Note: Rapid is relative to the consequences possible as opposed to an absolute time scale.*

### The First R – Resist

Critical infrastructure must be designed to resist attack and catastrophic failure. Immediately following the attacks and the subsequent collapse of the World Trade Center towers, there were those who called for high profile buildings and other critical infrastructure to be designed to stop airplanes. This, simply put, is utter nonsense. Unless we are prepared to live in a heavily engineered environment more closely resembling the complex of caves in Afghanistan, we will not design buildings to stop planes. To suggest so is a disservice to both our profession and to society in general. The challenge is to keep airplanes away from buildings and to root out those who challenge our way of life at the source.

But does that mean our profession is to do nothing? Far from it. Each “engineering” disaster, whether natural or manmade, has taught us lessons. Over time, these lessons are disseminated within a subset of our profession or within an industry segment. Some lessons are only understood

with the fullness of time and often offer a deeper understanding of the real challenges we as engineers face. Short-term code modifications often satisfy the tendency to over-react in the short term but, as understanding develops, may fail to sufficiently react in the longer term.

Our profession's tendency to specialize often constrains our ability to translate "lessons learned" across a broad range of disciplines and industry segments. Here, perhaps, lies a role for The Royal Academy of Engineering – to know all that is being done, to learn from an incident, to consolidate this invaluable source of knowledge and to insure its timely distribution across the industries. Perhaps the return of the Renaissance ideals embodied in the master builders are once again in order.

In New York on September 11<sup>th</sup> we saw the best of engineering, not the failure of it. We saw two proud structures swallow two maliciously guided planes that were fully loaded with fuel, and endure not only an impact beyond their design basis, but also an ensuing fire hotter and larger in scope. In the face of these attacks, these buildings did not simply allow themselves to be overwhelmed as the attackers most likely envisioned. Rather, they were the first of the many heroes to die that day, but only after they had bought the time for up to 25,000 to leave and live. This is the true testament to the designers of the structures, and our recognition of their successful resistance to an overwhelming attack in no way diminishes the human tragedy associated with those who did not safely escape that day.

In Washington, DC, we also saw the best of engineering, not the failure of it. The ability to withstand a direct deliberate assault on the scale we witnessed and to allow so many to survive speaks well of our profession's ability to design our critical infrastructure to resist. Our challenge as we move forward is to learn what we can from these tragedies and, as we have in the past, intelligently incorporate these lessons into our endeavors of the future. We must be comprehensive in our understanding, thorough in our consolidation of lessons learned and broader in our distribution, especially for those lessons that transcend specialties and industries.

Not all damage on September 11<sup>th</sup> was to the high-profile buildings in New York and Washington that filled our television screen. The damage to surrounding infrastructure – transport, electricity and telephone – exceeds that to the buildings in dollar terms. The very open role of infrastructure – to tie development together – in some ways limits its ability to resist deliberate attack. Infrastructure's limited ability to resist provides a sufficient segue to the second of the 3Rs of critical infrastructure.

### **The Second R - Respond**

The attacks of September 11<sup>th</sup> destroyed the operability of large portions of the transportation, electricity and telephone networks servicing lower Manhattan and impacted, more broadly, entire system operation. In the immediate aftermath of the attacks, transit system operators modified system operation to stop passenger flow into the affected area and to remove trains already in the area. That immediate action prevented any loss of life to transit passengers or workers despite the subsequent destruction of portions of the transit system from falling debris. But on the heels of that immediate response came an even more daunting challenge – to reconfigure the original transportation system to meet the needs of the 850 businesses and 125,000 workers physically displaced when 29 million square feet of office space was damaged or destroyed, and provide for

a reasonable restoration of service to the over 350,000 passengers to lower Manhattan who had their commuting patterns disrupted. Many valuable lessons learned for the highly engineered environment cities can be learned. These include:

- The link between infrastructure and development is crucial;
- “Core capacity” of infrastructure systems is essential;
- Deferred maintenance represents a real cost and a real risk;
- Operational and emergency response training is an integral element of critical infrastructure response; and
- Today’s highly engineered environment requires a first responder team that goes beyond the traditional triad of fire, police and emergency services.

**Lesson 1 – *Link between infrastructure and development highlighted***

I sometimes feel this has been a hobbyhorse of mine for too long. Infrastructure and development are intricately linked, often in ways we fail to fully appreciate. Each is the sine qua non of the other. Each of these “systems” is tightly coupled. However, as is often the case with all that we engineer, we can best appreciate the strengths, weaknesses and functionality only in their failure or application in response to some new paradigm.

September 11<sup>th</sup> highlighted the inter-relationships of infrastructure and development. In the “localized” failure of “development” (the collapse of the World Trade Center Towers), we witnessed a “localized” destruction of the attendant infrastructure (1 and 9 subway, local power grid, PATH station at WTC, etc.). In the reconfiguration of “regional development” (an estimated 29,000 employees working outside NYC as a result of September 11<sup>th</sup> and another 29,000 temporarily backfilled in other existing metropolitan-area space), we reconfigured our “regional” transportation network (mandatory HOV, increased ferry service, increased transit ridership at other river crossings, etc.). Similar analogs exist for utility and telecommunications networks affected on September 11<sup>th</sup>. However, this ability to reconfigure the infrastructure systems in response to a new development paradigm draws heavily from what we find in Lesson 2.

**Lesson 2 – *“Core capacity” of infrastructure systems is essential***

Earlier in 2001 I had the opportunity to attempt to explain the importance of some planned New York City transportation improvements to members of the political arena. The basic case I tried to make was that these improvements were about enhancing the core capacity of a well-developed transportation network in order to improve overall system reliability, availability and performance. By “core capacity” I’m referring to the degree of interconnectivity of the various elements of the system, as well as the number of alternative paths available...its flexibility and redundancy.

De facto, these additions to core capacity strengthened the overall system, going well beyond the benefits associated with new system connections from some new point A to new point B. To say my case for strengthening a complex system, inherently tying together the most complex and engineered urban environment in the world, was lost would be an overstatement...but not by much. Traditional project evaluation models focused on “new riders” from new connections between points A and B. But, in complex systems, the dislocations that can be caused by even a partial loss of overall system capacity and capability can be much more profound. Similarly, the improved reliability, availability and performance created by adding core capacity to a complex system can pay dividends not often easily seen.

Such was the case for the regional transit system in the aftermath of September 11<sup>th</sup>. The core capacity of these systems provided the flexibility to deal with commuting patterns literally modified overnight with lines and stations outside the immediately affected area, seeing changed passenger volumes exceeding those often associated with new point “A” to “B” connections. It was gratifying to receive the call from the political arena several days later stating that they now understood “core capacity”.

Each of the infrastructure systems impacted by September 11<sup>th</sup> responded more or less quickly depending on the core capacity inherently incorporated in the system as well as the concentration of critical infrastructure in the damaged area. Older systems tended to be more built out while many newer systems were still heavily focused on building new “A” to “B” connections and as such had not yet achieved the level of core capacity of some of the more mature systems. This suggests that core capacity needs to be a criterion as we plan and implement the new infrastructure the 21<sup>st</sup> century will undoubtedly require.

Complex systems need a new model. We must recognize that dislocations can be profound. We must also recognize that improved reliability, availability and performance pay hidden dividends.

Core capacity is not just about the extent of system or number of alternate system paths. It is also about the intrinsic quality of the system at the point in time when it is stressed. This brings us to the third lesson learned.

### ***Lesson 3 – Deferred maintenance represents a real cost and a real risk***

The history of our profession is marked by exciting breakthroughs, great works of master builders, and outstanding service to our nation’s and the world’s population. Regretfully, it is also marked by systemic degradation of some of our greatest achievements. As a society, and perhaps even in some parts of our profession, we do not see sustained maintenance as important as the creation of the next new grand work. Whatever the reason – its routine nature, the ability to hopefully do it tomorrow, the lack of technical complexity, or just plain lack of sex appeal – we are collectively guilty of allowing some of our most complex systems to fall into disrepair and to have their level of reliability, availability and operational and safety performance degraded. We have seen this most notably in failing rail systems in England and the U.S., but the impacts of deferred maintenance affect every element of infrastructure.

To a large measure the ability of New York City’s transit system to respond and to fully take advantage of the core capacity inherent in its system has its roots back at the time of the system’s nadir. Out of crisis emerged a commitment to fund, reorganize, rebuild, improve and maintain to a well-defined standard. This, too, stands as one of the lessons to recognize as we engineer and operate our increasingly complex infrastructure systems. The strength of a well-maintained system is clearly seen in the aftermath. Other elements of infrastructure with higher backlogs of deferred maintenance are struggling to keep up and for many the challenges are in the years immediately ahead.

The condition of the system, how well it is maintained, is critical to sustain its ability to respond. The backlog of deferred maintenance should be viewed as an element of systems risk. On September 11<sup>th</sup>, and in its aftermath, systems in a state of good repair fared better in both the response and recovery phases.

This ability to respond often to other than design basis events is key to the integrity of new security and safety systems.

**Lesson 4 – *Operational and emergency response training is an integral element of critical infrastructure response***

I won't belabor the point since in many ways I've made it in looking across the prior three lessons. Succinctly, in the same way we factor constructability reviews into our design process and maintainability considerations into our construction details, so must we address operational training as an element of our engineering of critical infrastructure. The events of September 11<sup>th</sup> show many areas of exceptional performance, but this serves to only underscore the importance of operational training. The operational training for the events of the 21<sup>st</sup> century changed after September 11<sup>th</sup>. New scenarios need to be considered. New threats in the form of weapons of mass destruction, higher risk of collateral physical and economic damage and more extended response timeframes need to be addressed. First responder training (actions, interactions, communications, decision making) needs to be integrated with infrastructure system operational training.

Simple items such as establishing evacuation routes and off-property staging areas must be clearly provided by the infrastructure of our built environment, but also must be clearly integrated in first responder protocols.

Scenario training must be evolutionary as new threats emerge. Emerging response plans must be reviewed regularly and revamped as needed. Unusual incident reporting must be similarly kept up to date and relevant. Training to handle a growing range of threat scenarios must be kept current.

On September 11<sup>th</sup> we saw the impact of having the Emergency Operation Center (EOC) in proximity to a high-profile target. We also saw the importance of having safe, redundant capability and comprehensive integration with other relevant EOCs. Quick response is essential and the importance of interoperability of first responders has not received as much attention in the past as might be currently warranted.

But we must not stop there. We must also understand how the first responder team has evolved in light of our increasingly engineered environment.

**Lesson 5 – *Today's highly engineered environment requires a first responder team that goes beyond the traditional triad of fire, police and emergency services***

In early 2001, I sat in the Engineering & Construction Governor's meeting of the World Economic Forum (WEF) in Davos, Switzerland. An earthquake had just struck India and one of the WEF governors was attempting to mobilize construction equipment to assist in rescue and recovery. Engineers and constructors were not viewed as traditional members of the emergency response team and the barriers to "doing the right thing" were immense. Out of that frustration grew the WEF Disaster Response Network.

On September 11<sup>th</sup> we witnessed the engineering and construction industry voluntarily reach out and provide the technical and construction expertise for one of the greatest disasters in a highly engineered environment. All necessary protocols were not firmly in place and response training had never fully factored this dimension in. Yet, this fourth responder will be even more critical as the 21<sup>st</sup> century unfolds.

While many good examples do exist, response protocols in our engineered urban environment will increasingly need to proactively incorporate this fourth responder. New, dedicated first responder training facilities reflecting the unique nature of highly engineered environments and their infrastructure need to be deployed, and legislation provided to remove the onerous risks that accrue to engineer volunteers who are often not covered by Good Samaritan statutes.

If we learn – and remember - each of these five lessons well, we will greatly enhance our ability to respond. But our ability to resist and respond in our critical infrastructure must also be matched by the third R, our ability to recover.

### **The Third R – Recover**

We design to resist, to avoid catastrophic failure in our critical infrastructure, to delay the failure as long as possible if it's not preventable, and to minimize loss of life, collateral damage, and degraded system performance. Having built in as much resistance as makes sense from a risk-weighted and operational and economic perspective, we enhance our ability to respond. We provide core capacity; we focus on reliability, availability and performance. We reconfigure inherently resilient systems for both the short- and the long-term.

But, for our critical infrastructure, that is not enough. We must recover the capacity and service that was destroyed. We must restore the engineered fabric, making it better than it was, if possible. We must engineer for recovery. From an engineering standpoint, this can mean many things:

- providing for accessibility to the sites of critical infrastructure;
- ensuring availability of specialized construction equipment, contracts and materials;
- developing a well-documented system with clear interface points; and
- preplanning and rehearsing response and recovery scenarios for high-probability events (earthquake, hurricane, flood in areas so prone).

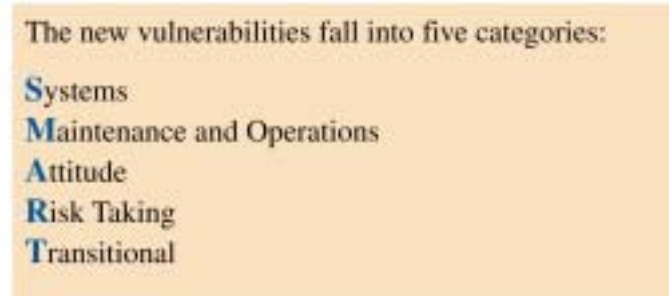
But, to truly respond in a highly engineered environment, even more is required. A vision must exist. Whether that notional concept of the master builder of the past or the well-developed consensus builder recent history has required is irrelevant. Each aspect of our engineered environment must be understood not only in terms of its past and present, but, perhaps more importantly, its future. How it will evolve. How resistance, response and recovery will be built in as the system expands. How it fits in that vision of the future. What role it provides as part of a larger engineered environment. It is only with this vision in hand that a clear unambiguous and deliberate recovery effort can begin.

### **Be SMART: The New Vulnerabilities**

The vulnerabilities of September 11<sup>th</sup> do not represent the full range of threats the future may hold for our cities and our critical infrastructure. The attraction to public infrastructure as a likely target is driven by the political statement it makes, the potential for destabilizing public confidence as well as the international recognition associated with higher profile targets. By its nature, infrastructure is an open system. Its accessibility is predictable, its demographics known and its behavior on a diurnal basis well established. It provides a target that by its very nature can cause maximum harm. We must be SMART about these vulnerabilities, which we may broadly group

into five types as shown in Table 3. The challenge is to build on the lessons learned on September 11<sup>th</sup> as previously described and to also consider other large-scale, systems scale, events.

*Table 3*  
**BE SMART**



The new vulnerabilities fall into five categories:

- Systems
- Maintenance and Operations
- Attitude
- Risk Taking
- Transitional

Consideration of each of these vulnerabilities and the lessons learned within the framework provided by the 3Rs provides a basis for reviewing the adequacy of existing infrastructure systems and planning their enhancement. They provide a framework for truly getting value for the money.

### **System Vulnerabilities**

The events of September 11<sup>th</sup> drive us to take a “systems perspective” when reviewing our critical infrastructure. Not surprisingly, the first set of vulnerabilities we need to be SMART about deal directly with the very nature of the system.

In particular, we need to understand the risks associated with:

1. *Failure to recognize the “built environment” as a growing and ever more complex system*  
This is perhaps the most fundamental risk we have. Development and infrastructure do not exist in isolation.
2. *Inadequate “system” understanding*  
It may not be rocket science, or a high-technology defense system, but it is no less important to understand what may go wrong, and how to detect and remedy it.
3. *Positive feedback loop risks*  
Also described as progressive failures, these considerations affect everything from the structural systems of a building, such as we saw induced by fire in the World Trade Center, to feedback mechanisms that degrade other elements of the system. This was seen in the need to relocate the Emergency Operations Center located at 7 World Trade Center.

4. *Centralized control weaknesses in complex systems*

There is a need for interoperability and an ability to see the situation. Partial decentralization of systems is required.

5. *“Tight Coupling” of systems*

Simply put, an event in one system leads to an event in another in short order. This was previously detailed in Lesson 1.

6. *Failing to KISS*

No, this is not the romantic in me, but rather the importance of “Keeping It Simple...Stupid.” We must recognize some classes of systems and certain technologies are inherently open to chains of failure. In such systems, adding additional safety systems only raises the level of complexity.

7. *Inadequate “core capacity”*

Lesson 2 highlighted the importance of interconnectivity, flexibility and redundancy to system responsiveness to unplanned events. Core capacity was a major factor in New York’s transit systems being able to restructure themselves immediately following September 11<sup>th</sup>.

All too often we emphasize “reach” (new customers) over “responsiveness” when making key decisions regarding our infrastructure investment.

Consideration of these vulnerabilities will enhance the resiliency of critical infrastructure. Those systems that more fully addressed these considerations responded better on September 11<sup>th</sup>.

**Maintenance and Operation Vulnerabilities**

If system vulnerabilities focus on ensuring that the right system is put in place, then maintenance vulnerabilities are focused on keeping it that way.

Specific risks include:

1. *Failing to recognize the importance of state of good repair*

We saw this in Lesson 3. Those infrastructure systems in a state of good repair suffered less collateral effects when a portion of the system was stressed to failure.

There will be a tendency to compensate for maintenance and operational vulnerabilities by adding on top of the existing base system. In complex systems, in particular, this can act to create new risks. The foundation must be strong.

2. *Inadequate renewal of emergency training*

The systems of our built environment are not static, nor are the threats they face. Emergency training must be undertaken recognizing the dynamic environment within which our built environment exists as well as its own inherently dynamic nature.

3. *Inadequate operating provisions to limit disturbances*

Failure must be contained or localized to prohibit “tight coupling” effects from taking hold. In New York on September 11<sup>th</sup> we saw operating action take preventive steps against further

failure of the PATH and NYC Transit lines as a result of flooding in damaged sections. In more routine circumstances we find good examples in power-grid inter-ties.

### **Attitude Vulnerabilities**

In contrast with system and maintenance vulnerabilities that focus on whether the right system is in place and whether it's sustained properly, attitude vulnerabilities address our willingness to accept an unexpected or undesired truth. Specific attitude risks include:

#### 1. *Cognitive lock*

In life, particularly when we are under stress, we expect certain situations to evolve in certain ways. Sometimes they don't. Cognitive lock occurs when we hold onto a course of action against all contradictory evidence. This can be particularly disastrous when combined with a complex system and often requires a fresh pair of eyes to see the new "truth" in front of us. I include haste as an attitude vulnerability given the risks often incurred, unknowingly, when blindly charging ahead.

#### 2. *Over-commitment to bureaucratic goals*

The goal has been set and any deviation from the goal is not acceptable. Problems that arise are ignored if they put the goal at risk. The unmovable goals set for aviation security ignored the realities of having a comprehensive approach in favor of meeting a fixed end date. Does mere achievement of the bureaucratic goal ensure we have accomplished our true aim?

#### 3. *Prisoner to Heuristics*

Past experience or what we've heard prevents us from taking a broader look. We adopt a perspective of "it never happened, so it's not credible." When the command center was established at the World Trade Center on September 11<sup>th</sup>, it was set up in the shadow of the unstruck south tower. The possibility of a deliberate attack on two (or more) buildings at the same time in a way designed to cripple first responder capability was not considered credible.

Being a prisoner to heuristics also involves a failure to consider what we see or learn from analogous systems or settings. Are multiple, simultaneous attacks, or attacks on first responder teams the new norm? Or do we run the risk of the next attitude vulnerability?

#### 4. *Denial*

Conventional threat analysis has us consider a range of likely scenarios and design our systems to resist, respond and recover from such scenarios. But the unlikely is also possible and it, too, must be considered. How do you address these unlikely scenarios in your system design and operation? At one level you can't because one can always postulate another unlikely scenario that will defeat any specific system measures you undertake. So what is one to do?

In many ways this brings us full circle to the need to have inherently flexible, redundant and reliable systems. Core capacity provides the trained system operator with the tools to address a broad range of unlikely scenarios.

Contingency planning for our critical infrastructure must include training in the capabilities and limits of various system elements. The unlikely must be part of our planning processes.

## 5. *Failure to learn “lessons learned”*

Over the last year I’ve tried to distill down the events of September 11<sup>th</sup> into a set of factors for us to consider in the future design and operation of our critical infrastructure. These lessons are not unique to the events of September 11<sup>th</sup>. Rather, from an engineering standpoint, we have seen many of these lessons learned in prior events of scale in heavily engineered systems.

### **Risk-taking Vulnerabilities**

None of us likes to be wrong. But the way we perceive risks and handle mistakes affects the range of actions we are willing to consider when faced with extreme situations. Two particular risk-taking vulnerabilities are worth calling out.

#### 1. *Litigation constrains risk-taking in the respond and recover phases*

All evidence points to the engineer and constructor increasingly being part of tomorrow’s first responder team in our heavily built environment. This was one of these lessons learned on September 11<sup>th</sup>. But while the engineering profession responded, voluntarily and overwhelmingly, it did so at its own peril. As licensed professionals undertaking their profession, it was not clear whether they were covered by Good Samaritan legislation. How will they behave next time if a lawsuit is filed for a “mistake” they made while trying to help others?

#### 2. *Fear of “satisficing”*

We are often called to make decisions or take actions in the absence of complete information. Our willingness to take action and move forward with an apparently workable solution is often a function of how mistakes are perceived and handled.

Running heavy cranes out across the debris field following the collapse of the World Trade Center was an example of willingness to “satisfice.” No as-builts existed and a high degree of judgment and risk-taking was required. How might we have handled a mistake that sent a crane toppling or crashing through the sub-basement structure?

### **Transitional Vulnerabilities**

Change is the watchword of life. In the aftermath of September 11<sup>th</sup> we will seek to improve what we do, add new levels of safety, change protocols, etc. But in the process we must recognize that complex infrastructure systems, and, for that matter, systems in general, are often most vulnerable immediately before, during and immediately after this change process. What are some of these transitional vulnerabilities and what must we be cognizant of as we move through these transition stages? They include:

#### 1. *Inadequate use of currently deployed resources*

There is a tendency to look for the “silver bullet” as opposed to better deploying and applying the resources at hand.

#### 2. *Change processes further stress existing systems*

These risks are today’s issues as we modify our air travel regimes, handling of “just-in-time” commerce and revamp first responder efforts. Change for change’s sake is not necessarily the answer and, approached narrowly, may increase the overall risks we face.

3. *New system failure rates not planned*

True operating characteristics and failure rates of new systems can only be understood after an extended period of operating under both good and bad conditions. The old adage that you “don’t know what you don’t know” is particularly relevant during a transitional period.

4. *Technology put ahead of people*

September 11<sup>th</sup> taught us that people cannot, nor should not, be taken out of the loop. It was individual actions that led to the shutdown of transit lines...not technology. It was individual action that dispatched ferries, buses, generators, cranes and engineers...not technology. Technology is a powerful enabler of people...but it needs to fit them, not the other way around.

We’ve looked back at some of the lessons we should learn from September 11<sup>th</sup> and looked around at what experiences from other systems failures have taught us so we may better understand the full range of vulnerabilities our critical infrastructure faces. But what are the challenges ahead?

**Challenges Ahead**

The challenges ahead for critical infrastructure are best viewed from our perspective of the 3Rs – Resist, Respond, Recover. From this perspective, challenges fall into four categories, two associated with the resistance phase and one each for the respond and recover phases. These four types of challenges relate to:

- Systems whose rapid failure would lead to catastrophic loss of life
  - Type 1 – Resistance (Life)
- Systems whose failure would lead to unacceptable economic consequences
  - Type 2 – Resistance (Economic)
- Systems whose failure would significantly impact rescue and response efforts
  - Type 3 – Response
- Systems whose degradation would significantly impact recovery efforts
  - Type 4 – Recovery

Table 4 looks ahead and provides a framework for moving from our definitions for critical infrastructure, through the lessons learned from September 11<sup>th</sup> and other similar catastrophic system events, to those areas requiring our attention as we move forward. I’ve not detailed specific issues or recommendations in this lecture, but have previously enumerated a number of these areas.

**Table 4**  
**Critical Infrastructure Challenges Ahead: A 3R Perspective**

Resistance Challenges – Type 1 (Life)
<ul style="list-style-type: none"> <li>• <b>Asymmetric threats (weapons of mass destruction)</b> <ul style="list-style-type: none"> <li>◦ Externally introduced               <ul style="list-style-type: none"> <li>• <i>Seaports</i></li> <li>• <i>Border crossings</i></li> </ul> </li> <li>◦ Externally introduced               <ul style="list-style-type: none"> <li>• <i>Airports</i></li> <li>• <i>Nuclear/chemical plants</i></li> <li>• <i>Major public spaces – transport terminals/hubs/large public gathering spaces</i></li> <li>• <i>Water supply</i></li> </ul> </li> </ul> </li> </ul>
Resistance Challenges – Type 2 (Economic)
<ul style="list-style-type: none"> <li>• <b>Single point failure threats (conventional or unconventional weapons)</b> <ul style="list-style-type: none"> <li>◦ Major infrastructure links with:               <ul style="list-style-type: none"> <li>• <i>Extended repair times or costs</i></li> <li>• <i>Limited or no alternate “system” connections</i></li> <li>• <i>Broad “system” degradation potential</i></li> </ul> </li> <li>◦ Particularly at risk are:               <ul style="list-style-type: none"> <li>• <i>Major river crossings</i></li> <li>• <i>Underground, urban links</i></li> </ul> </li> </ul> </li> <li>• <b>Degraded ubiquitous infrastructure system control/capability (conventional or unconventional weapons, cyber or insider threat)</b> <ul style="list-style-type: none"> <li>◦ Major control centers and functionality</li> </ul> </li> <li>• <b>Trade interruption or degraded trade system</b> <ul style="list-style-type: none"> <li>◦ Major port facilities               <ul style="list-style-type: none"> <li>• <i>cargo and energy</i></li> </ul> </li> <li>◦ Increased supply-chain transit times due to increased security requirements</li> </ul> </li> </ul>
Response Challenges – Type 3
<ul style="list-style-type: none"> <li>• <b>First responder protection &amp; interoperability</b> <ul style="list-style-type: none"> <li>◦ Equipment &amp; training for fuller range of threats</li> <li>◦ Mission reliable communications</li> <li>◦ Enhanced communication at responder level between first responder elements</li> <li>◦ Enhanced rapid toxin identification</li> </ul> </li> <li>• <b>Emergency operation center survivability</b> <ul style="list-style-type: none"> <li>◦ Enhanced site selection &amp; screening</li> <li>◦ Hardening and protection for EOC sites &amp; facilities</li> </ul> </li> </ul>
Recovery Challenges – Type 4
<ul style="list-style-type: none"> <li>• <b>Inadequate specialized personnel, facilities and equipment</b> <ul style="list-style-type: none"> <li>◦ Needs not well defined in homeland security context</li> </ul> </li> <li>• <b>Inadequate legislative, financial, contracting and risk management framework</b></li> </ul>

### **Where We Are Today**

It has been a little over a year since the terrorist attacks of September 11<sup>th</sup> and the recovery process is well underway. In New York, the subway line has been restored and work is well underway to put the World Trade Center station back into temporary service and reopen the rail river crossing that has been out of service. In Washington, DC workers have already reoccupied offices at the point of impact, in the Pentagon's outermost ring.

Nationwide, the focus on identifying and defining critical infrastructure has begun. In New York, Washington and other major urban centers, we are addressing the need for resistance. While much has been done, much more still needs to happen.

The first lesson learned on September 11<sup>th</sup>, namely the strong linkage between infrastructure and development, has been truly learned in New York as redevelopment planning considers its respective needs in an integrated fashion.

Similarly, the recognition of the role of "core capacity" in infrastructure systems has been highlighted. The decisions to proceed with additional linkages in the rail network ("7" train extension; 2<sup>nd</sup> Avenue Subway) will only reinforce the core capacity that existed prior to September 11<sup>th</sup>.

The risks associated with deferred maintenance, the third lesson learned, were called home as AMTRAK reached a financial crisis and money was invested by the federal government in maintenance and renewal of critical infrastructure. More yet remains to be done, however.

In New York, Washington and other major urban centers, the focus on operational and emerging response training has increased, although the full benefit of these programs is still some years off. Inter-operability of first responders is currently the focus of the CAPWIN project in Washington.

But the last of our five principal lessons learned on September 11<sup>th</sup> still appears to be struggling. The role of the engineer as part of first responder efforts in our increasingly built environment has not yet been realized. It is here that groups such as The Royal Academy of Engineering can make a difference.

We have learned much, but we must learn more. Just as the 3Rs provided the foundation for our expanding knowledge base as individuals, so, too, must the 3Rs of critical infrastructure be learned so our cities, development and infrastructure together, can expand to meet the needs of our society in the years ahead.

## The Royal Academy of Engineering

The objectives of The Royal Academy of Engineering are to pursue, encourage and maintain excellence in the whole field of engineering in order to promote the advancement of the science, art and practice of engineering for the benefit of the public.

The Academy comprises the United Kingdom's most eminent engineers of all disciplines. It is able to take advantage of their wealth of knowledge and experience which, with the interdisciplinary character of the membership, provides a unique resource with which to meet the objectives.

Its activities include an extensive education programme, research chairs and fellowships, visiting professorships, industrial secondments and international travel grants. It provides expert advice on engineering matters to government and other bodies and awards the UK's premier annual prize for innovation in engineering, The Royal Academy of Engineering MacRobert Award.

Election to The Academy is by invitation only. Up to sixty Fellows may be elected annually, together with Honorary Fellows and Foreign Members who have made exceptional contributions to engineering. All are elected by their peers for personal achievement of exceptional merit and distinction. Fellows are distinguished by the title "Fellow of The Royal Academy of Engineering" and use the designatory letters "FREng".

The Academy was founded in 1976 as The Fellowship of Engineering on the initiative of HRH The Duke of Edinburgh and a group of distinguished engineers. It was granted its Royal Charter in 1983 and, with the consent of HM The Queen, adopted the present title in 1992.

The Royal Academy of Engineering  
29 Great Peter Street, Westminster, London SW1P 3LW  
Telephone: 020 7222 2688 Facsimile: 020 7233 0054  
Website: [www.raeng.org.uk](http://www.raeng.org.uk)  
Registered Charity No. 293074