The
BRIDGE

NATIONAL ACADEMY OF ENGINEERING

Editor-in-Chief

The Bridge (USPS 551-240) is published quarterly by the National Academy of Engineering, 2101 Constitution Avenue, N.W., Washington, DC 20418. Periodicals postage paid at Washington, D.C.

Vol. 32, No. 1 Spring 2002

Postmaster: Send address changes to *The Bridge*, 2101 Constitution Avenue, N.W., Washington, DC 20418.

Papers are presented in *The Bridge* on the basis of general interest and timeliness. They reflect the views of the authors and do not necessarily represent the position of the National Academy of Engineering.

The Bridge is printed on recycled paper. ♻

A complete copy of each issue of *The Bridge* is available in PDF format at http://www.nae.edu/TheBridge. Some of the articles in this issue are also available as HTML documents and may contain links to related sources of information, multimedia files, or other content.

The BRIDGE
Volume 32, Number 1 • Spring 2002
LINKING ENGINEERING AND SOCIETY

Editorial

Features

(continued on next page)

THE NATIONAL ACADEMIES

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Bruce M. Alberts is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. Wm. A. Wulf is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Kenneth I. Shine is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Bruce M. Alberts and Dr. Wm. A. Wulf are chairman and vice chairman, respectively, of the National Research Council.

Editorial

George Bugliarello is chancellor of Polytechnic University in Brooklyn, N.Y.

Engineering and Homeland Defense

Since time immemorial, warfare has been shaped by technology and by the interplay of defense and offense. The events of September 11 have opened a new chapter in this saga. The question of homeland security is not new. It has been addressed in the context of the Cold War and of potential threats from rogue nations. But the events of September 11 focused national attention on the reality, urgency, and hydra-like nature of the terrorist threats confronting the United States. A nation confident in its openness has, for the first time in its history, experienced terrorism on a large scale and must now prepare itself for the possibility of ubiquitous threats to its infrastructure and the lives of its citizens. Every citizen is now on the front line.

We may never be able to prevent all attacks, but we can endeavor to reduce their probability and potential consequences. Terrorist attacks present enormous engineering challenges in information gathering, in data mining, in sensing, in cybercommunications and telecommunications, in the security of transportation systems and water, energy, and food supplies, in the management of emergencies and the rapid evacuation of people, in the design and retrofitting of structures, in firefighting, in identification technologies, and in reducing biohazards and other threats of mass destruction. This issue of *The Bridge* addresses some of these challenges and some of the vulnerabilities that have emerged since September 11, which are heightened by the complex interdependencies of our infrastructural systems.

The engineering enterprise, which has built the sinews of an open and trusting society, must now help protect it from the insidious forces that want to destroy it. This will require that we rethink our ideas about engineering. For instance, in the design and operation of infrastructure, we need to consider not only capacity and reliability and cost, but also the ability to withstand terrorist attacks, or at least to mitigate their consequences. Much technology is already available that can immediately be brought to bear on these challenges. Other technology needs to be developed urgently. But the tasks must be prioritized in terms of risk. Not everything can be protected. This calls for a realistic assessment of what can be done, in the short term and in the long term, and of the cost effectiveness of proposed measures in terms of the risks they address.

We must identify and concentrate our attention on technological bottlenecks, such as adequate sensors, our ability to inspect from a distance ships entering a harbor, and our ability to locate victims buried in rubble or guide a firefighter through smoke in the interior of a building. These are all engineering challenges of the first order. There is a huge need to provide training in the most effective use of new technologies and to educate architects, engineers, urban planners, and infrastructure managers to the new realities. Things have changed. Cities, which in the past provided an element of protection to their inhabitants, today, as in World War II, have become prime targets, but in a different way. The tallest buildings and the longest bridges, the pride of our cities and our society, are now magnets for attack. We need to reevaluate the ultralight construction that made them possible and economical and reconsider their design. We also need to study the lessons we have learned from terrorist attacks here and abroad. For instance, one painful lesson, made clear by the consequences of the concentration of telecommunications infrastructures in the World Trade Center area in New York, is the need for redundancies and decentralization. Another is the importance of wireless communications as alternative channels of communication.

We need to consider not only how to protect our vital systems, but also how to restore them rapidly after an event that we might not be able to avoid. In terms of risk and priorities, bioterrorism is far more insidious than chemical terrorism and deserves a very high priority. So does, in our information society, the question of cyber security, as the penetration or interruption of our information networks by a determined adversary can do immense damage. Consider, for example, the catastrophic effects of a disruption to our financial system. Another imperative is the safety of the supply lines that bring food, materials, and goods to our population from

all over the globe, as well as from within the United States. At this moment, the U.S. Customs, the Food and Drug Administration, and the U.S. Department of Agriculture can test only between 1 and 2 percent of the material that enters the country through harbors, airports, and highways.

As new technologies are being developed to address these problems, we must remain extremely sensitive to issues of civil liberty and privacy. By necessity, some approaches will require the surrender of some of our traditional rights and changes in what we are accustomed to. For instance, the public must be educated to the fact that in the identification of terrorists or of the threat of a biological or chemical attack, false negatives are ultimately of greater concern than false positives. But effective technologies can greatly reduce the inconveniences caused by the latter.

These enormous challenges will demand a continuous dialogue between engineers and the larger community and the development of new partnerships between industry, government at all levels, universities, and research laboratories. Engineers are a key resource in our response to the imperatives of homeland defense, as well as in keeping our economy strong and productive.

George Bugliarello

The lead structural engineer reflects on the rise and fall of the World Trade Center towers.

Reflections on the World Trade Center

Leslie E. Robertson is a member of the NAE and director of design at Leslie E. Robertson Associates, R.L.L.P.

Leslie E. Robertson

The journey toward the design and construction of the World Trade Center began prior to 1960 when Minoru Yamasaki Associates was selected to design the Federal Science Pavilion, a key element of the Seattle World's Fair; NBBJ was selected as the local architect. Having accomplished many structural designs for NBBJ, it was only natural that we would obtain the commission for the structural design of the Pavilion. That structural design, reflecting the very highest attainments of our profession, was creatively conceived and executed by John V. Christiansen (NAE). Indeed, the Pavilion stands today as an example of the importance of fine structural engineering as it influences the overall architectural process. The entrepreneurship and skills of another of our partners, John B. Skilling (NAE), were instrumental in the development of the close relationship between our firm and that of Minoru Yamasaki and Associates; many wonderful projects were to follow.

When Yamasaki was commissioned to design the World Trade Center in New York, he proposed that we be retained as structural engineers. Although his recommendation was influential, we were in competition with many New York firms that had more experience in high-rise design than we had. Although we worked hard preparing for our interview with the Port Authority of New York and New Jersey, we wouldn't have obtained the commission without the presence and the skills of John Skilling.

Once we had been awarded the commission, I moved from Seattle to New

York with a team of expert engineers—Wayne A. Brewer (drawing production and coordination), Paul S.A. Foster (towers), Ernest T. Liu (plaza buildings and below-grade structures), Jostein Ness (detailing), Richard E. Taylor (computers), and E. James White (construction technology). Professor Alan G. Davenport (NAE), on sabbatical from the University of Western Ontario, joined us to head the wind-engineering research group. Although I was the titular leader, the energies and talents of the entire team led to our successes.

A list of the innovations incorporated into the World Trade Center would be very long. In the following pages, I describe just a few of the ideas and innovations conceived and developed by our team. Most, if not all, of this technology is now a part of the standard vocabulary of structural engineers.

The tubular framing system for the perimeter walls resisted all of the lateral forces imposed by wind and earthquake, as well as the impact loads imposed on September 11. Although we had used closely spaced columns in an earlier building, it was Minoru Yamasaki who proposed that we use narrow windows in the WTC towers to give people a sense of security as they looked down from on high. Our contribution was to make the closely spaced columns the fundamental lateral-force-resisting system for the two towers. The tubular framing system also precluded the need for the customary 30-foot column spacing in interior areas, making column-free, rentable space structurally desirable.

In support of Yamasaki's design, during the construction, before the windows were installed, I noticed that people felt comfortable walking up to the outside wall, placing their hands on the columns to either side, and enjoying the wonderful view. If the wind was blowing toward them, they would walk right up to the outside wall; however, if they felt even a trace of pressure from a breeze from behind, they would at least hesitate before walking to within five feet of the wall . . . and many would not approach the wall at all.

Another structural innovation was the outrigger space frame, which structurally linked the outside wall to the services core. This system performed several functions. First, gravity-induced vertical deformations between the columns of the services core and the columns of the outside wall were made equal at the top of the building; at other levels, the differential deformations were ameliorated. Second, wind-induced overturning moments were resisted in part by the columns of the services core, thus providing additional lateral stiffness. Finally, the weight

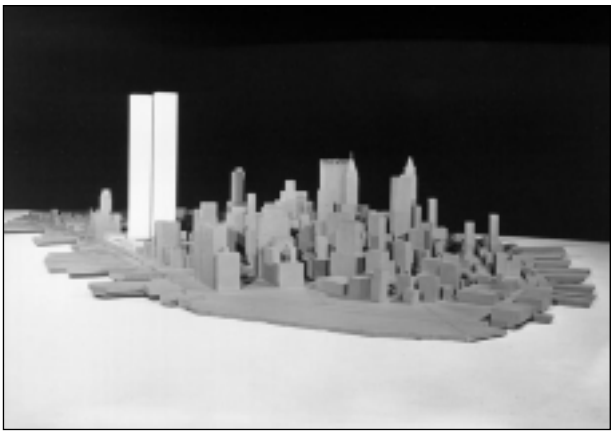

FIGURE 1 Wind tunnel model of the World Trade Center towers.

of, and the wind-induced overturning moment from the rooftop antenna (440 feet tall) was distributed to all columns in the building . . . adding additional redundancy and toughness to the design.

Prefabricated structural steel was used to an unprecedented degree. Two examples will give you an idea. Exterior wall panels three stories high and three columns wide were fabricated in Washington state. Floor panels 60 feet long and 20 feet wide, complete with profiled metal deck and electrical distribution cells, were assembled in New Jersey from components fabricated in Missouri and elsewhere.

We mounted a comprehensive program to determine the design-level gradient wind speed for New York City. Data were collected from all available sources and incorporated into an appropriate mathematical model. For the first time, we were able to obtain full-scale measurements of the turbulent structure of the wind and compare them with the turbulent structure obtained in a boundary-layer wind tunnel. This was done by mounting anemometers atop three high points in lower Manhattan and by making similar measurements on our wind tunnel model (Figure 1). The boundary-layer wind tunnel was further developed and used to predict the steady-state and dynamic forces on the structure and the glazing, as well as to develop the dynamic component of wind-induced motion of the structure. Jensen and Frank, two brilliant Danish engineers, had discovered that surface roughness in the wind tunnel allowed them to accurately predict wind pressures on farm structures. We expanded this technology upward to 110 stories by using a wind tunnel, constructed under the guidance of Dr. Jack E. Cermak, (NAE, Colorado State University), designed to study the dispersion of gases emitted from

tall stacks. Thus, for the first time, we were able to analyze the steady-state and dynamic components of wind-induced structure deflections.

We designed motion simulators to determine acceptable levels of wind-induced structure motion. The simulators measured the response of human subjects to lateral motions similar to those anticipated for the two towers. The accumulated data were used to establish the criteria for an acceptable level of the swaying motion of the two towers.

A viscoelastic damping system was invented and patented to ameliorate the wind-induced dynamic component of building motion by dissipating much of the energy of that motion . . . acting more or less like shock absorbers in an automobile. With these dampers, we could control the swaying motion without having to use large quantities of structural steel. This was the first time engineered dampers were used to resist the wind-induced swaying motion of a building.

A theory was developed for integrating the statistical strength of glass with the dynamic forces of the wind to predict the breakage rate of the glass of the exterior wall. Coupled with a testing program of actual glass samples, we were able to determine rationally the necessary thickness and grade of the glass. Another theory was developed to predict stack action and temperature-induced and wind-induced airflow within a high-rise building; an understanding of these airflows is crucial to controlling fire-generated smoke and reducing the energy consumption of the building. A theory to predict appropriate "parking floors" for elevators was developed to minimize the oscillation of elevator cables, which oscillation is stimulated by the wind-induced, swaying motion of a building. Figure 2 is a comparison of the wind-induced dynamic components of the structure response of the two towers and of the Empire State Building.

The two towers were the first structures outside of the military and nuclear industries designed to resist the impact of a jet airliner, the Boeing 707. It was assumed that the jetliner would be lost in the fog, seeking to land at JFK or at Newark. To the best of our knowledge, little was known about the effects of a fire from such an aircraft, and no designs were prepared for that circumstance. Indeed, at that time, no fireproofing systems were available to control the effects of such fires.

We developed the concept of and made use of the fire-rated shaft-wall partition system, which is now widely used in place of masonry and plaster walls. At that time, masonry was the standard enclosure for elevators, stairs, duct shafts, and other internal structures. The partition system eliminates the need for within-the-shaft scaffolding, which was the common practice, provides more smoke-proof stairs and shafts, and improves safety on the job site. The shaft-wall completely changed the nature of the structural system for the two towers, making them the first of a new kind of high-rise building.

A computerized system was conceived and developed for ordering structural steel and producing shop drawings for structural steel, as well as the operation of digitally directed tools, all directly from digital information developed as a part of our design.

When the two towers were finished, the World Trade Center stood proud, strong, and tall. Indeed, with little effort, the towers shrugged off the efforts of terrorist bombers in 1993 to bring them down. The events of

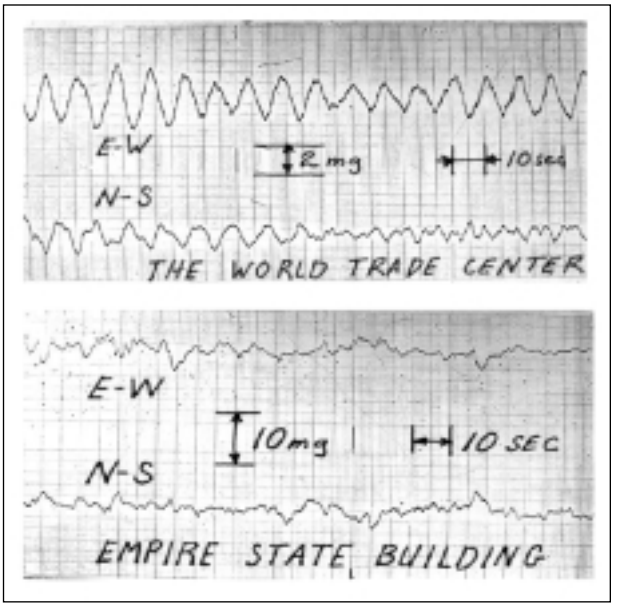

FIGURE 2 Comparison of the wind-induced dynamic components of the structure response of the World Trade Center towers and the Empire State Building.

September 11, however, are not well understood by me . . . and perhaps cannot really be understood by anyone. So I will simply state matters of fact:

The events of September 11 ended the lives of almost 2,900 people, many of them snuffed out by the collapse of structures designed by me. The damage created by the impact of the aircraft was followed by raging fires, which were enormously enhanced by the fuel aboard the aircraft. The temperatures above the impact zones must

have been unimaginable; none of us will ever forget the sight of those who took destiny into their own hands by leaping into space.

It appears that about 25,000 people safely exited the buildings, almost all of them from below the impact floors; almost everyone above the impact floors perished, either from the impact and fire or from the subsequent collapse. The structures of the buildings were heroic in some ways but less so in others. The buildings survived the impact of the Boeing 767 aircraft, an impact very much greater than had been contemplated in our design (a slow-flying Boeing 707 lost in the fog and seeking a landing field). Therefore, the robustness of the towers was exemplary. At the same time, the fires raging in the inner reaches of the buildings undermined their strength. In time, the unimaginable happened . . . wounded by the impact of the aircraft and bleeding from the fires, both of the towers of the World Trade Center collapsed.

Figure 3 shows the comparative energy of impact for the Mitchell bomber that hit the Empire State Building

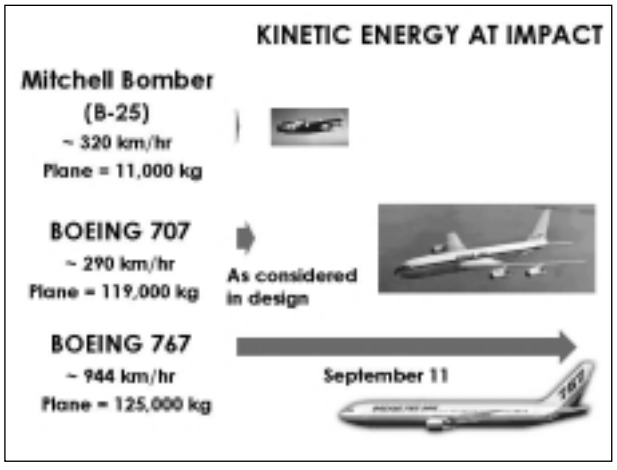

FIGURE 3 Kinetic energy at impact for various aircraft.

during World War II, a 707, and a 767. The energy contained in the fuel is shown in Figure 4. Considerations of larger aircraft are shown in Figures 5 and 6. The physical sizes of these aircraft are compared with the size of the floor plate of one of the towers in Figure 7. These charts demonstrate conclusively that we should not and cannot design buildings and structures to resist the impact of these aircraft. Instead, we must concentrate our efforts on keeping aircraft away from our tall buildings, sports stadiums, symbolic buildings, atomic plants,

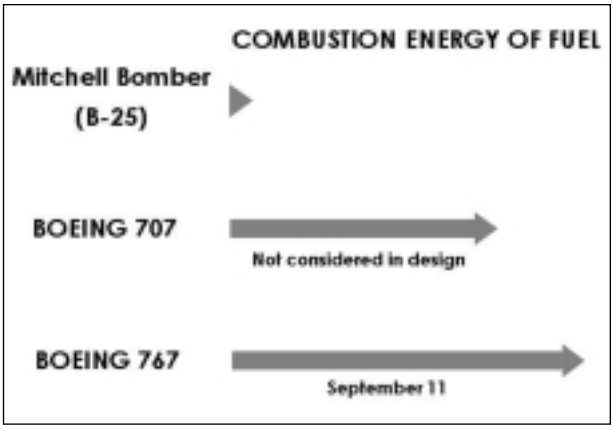

FIGURE 4 Combustion energy of fuel for various aircraft.

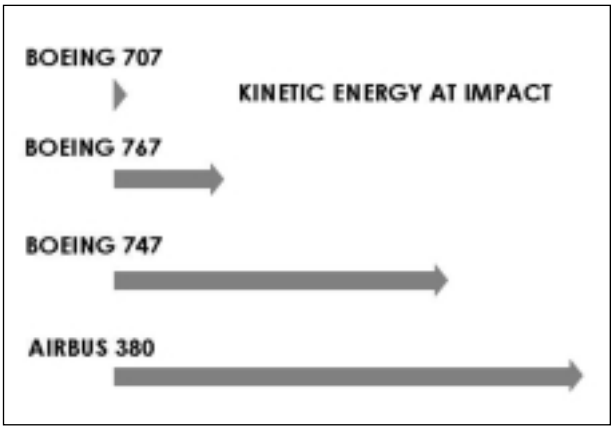

FIGURE 5 Kinetic energy at impact for various aircraft.

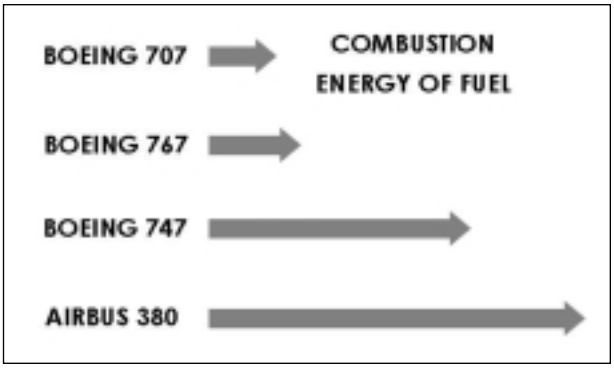

FIGURE 6 Combustion energy for fuel for various aircraft.

and other potential targets.

The extent of damage to the World Trade Center is almost beyond comprehension. Figure 8 shows an overview of the site and the location of the various buildings. We did not design the superstructures of Building 3 (Marriott Hotel) or of Building 7. Towers 1

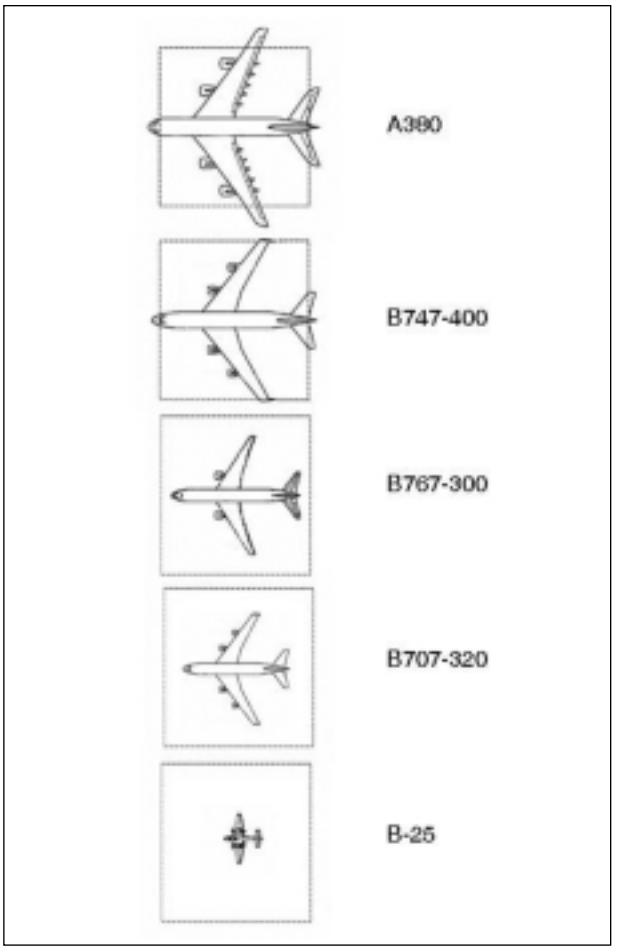

FIGURE 7 Comparison of the physical sizes of various aircraft with the size of the floor plate of one of the World Trade Center towers.

and 2, which were totally destroyed, left behind utter chaos surrounded by towers of naked structural steel. The remaining steel towers were in some ways painful beyond belief, in other ways strangely beautiful. Building 3 collapsed down to a structural transfer level designed by us. Fortunately, the people who sought refuge in the lobby of the hotel, which was located immediately below the transfer level, survived. Buildings 4, 5, and 6 remained standing but were partially collapsed by falling debris; all three burned for about 24 hours. Although there was nothing special about the structural design of these buildings, the remaining structures stalwartly resisted the impacts of the wrecking ball. Building 7, after burning for nearly 10 hours, collapsed down to a structural transfer level designed by us. The below-grade areas under Towers 1 and 2 were almost totally collapsed; in areas outside of the towers they were partially damaged or collapsed.

In my mind, the loss of life and the loss of the buildings are somehow separated. Thoughts of the thousands who lost their lives as my structures crashed down upon them come to me at night, rousing me from sleep, and interrupting my thoughts at unexpected times throughout the day. Those who were trapped above the impact floors, those who endured the intense heat only to be crushed by falling structure, are merged with those who chose to take control of their own destinies by leaping from the towers.

The loss of the buildings is more abstract. The buildings represented about 10 years of concerted effort both in design and in construction on the part of talented men and women from many disciplines. It just isn't possible for me to take the posture that the towers were only buildings . . . that these material things are not worthy of grieving.

It would be good to conclude this journey in a positive mode. We have received almost a thousand letters, e-pistles, and telephone calls in support of our designs. The poignant letters from those who survived the event and from the families of those who both did and did not survive cannot help but bring tears to one's eyes. They have taught me how little I know of my own skills and how fragile are the emotions that lie within me. Yes, I can laugh, I can compose a little story . . . but I cannot escape.

Do those communications help? In some ways they do; in others, they are constant reminders of my own limitations. In essence, the overly laudatory comments only heighten my sense that, if I were as farseeing and

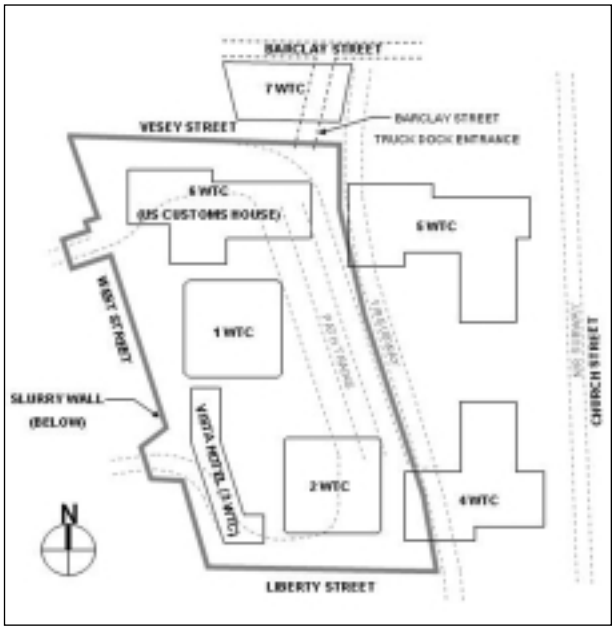

FIGURE 8 Overview of the World Trade Center site.

talented as the letters would have me be, the buildings would surely have been even more stalwart, would have stood even longer . . . would have allowed even more people to escape.

Yes, no doubt I could have made the towers braver, more stalwart. Indeed, the power to do so rested almost solely with me. The fine line between needless conservatism and appropriate increases in structural integrity can only be defined after careful thought and consideration of all of the alternatives. But these decisions are made in the heat of battle and in the quiet of one's dreams. Perhaps, if there had been more time for the dreaming . . .

Recognition must be given to the Port Authority of New York and New Jersey, who provided unparalleled support and guidance throughout the design and construction of the World Trade Center. Their understanding of the need to explore new avenues and break new ground reflected their sound professional and technical posture. We could not have asked for a more competent, more responsible, or more involved client. The men and women of our company who participated in the design and construction are without parallel. Their talents, energies, and good humor carried us through a most arduous journey. Dr. Alan G. Davenport (NAE) provided invaluable knowledge, insight, and support; his willingness to join us on this journey made many facets of the design possible. Minoru Yamasaki and his team, particularly Aaron Schreier, and the office of Emery Roth and Sons produced a wonderful architecture while making the entire process both fun and exciting. Richard T. Baum (NAE), of Jaros, Baum & Bolles, headed the HVAC (heating, ventilation, air conditioning) team and taught me much about these systems. Joseph R. Loring provided full professional services as the electrical engineer for the project.

In conclusion, the events of September 11 have profoundly affected the lives of countless millions of people. To the extent that the structural design of the World Trade Center contributed to the loss of life, the responsibility must surely rest with me. At the same time, the fact that the structures stood long enough for tens of thousands to escape is a tribute to the many talented men and women who spent endless hours toiling over the design and construction of the project . . . making us very proud of our profession. Surely, we have all learned the most important lesson—that the sanctity of human life rises far above all other values.

The engineer who oversaw the construction of the World Trade Center "bathtub" describes the recovery efforts.

World Trade Center "Bathtub": From Genesis to Armageddon

George J. Tamaro is a member of the NAE and senior partner, Mueser Rutledge Consulting Engineers.

George J. Tamaro

My first experience with "slurry wall" construction[1] was in Italy in 1964 when I was on a work/study assignment for the New York Port Authority. The Chief Engineer of the Port Authority at the time asked that I inspect and report to him on the use of the new technology. In 1967 the Port Authority assigned me to oversee the original construction of the World Trade Center (WTC) slurry walls. From that assignment I moved on to a nine-year career as a contractor constructing slurry walls and a 21-year career as a consulting engineer designing slurry walls around the globe. Back in 1964, I had no idea that my brief assignment in Rome would have a significant effect on my career and interests. This report describes the initial work on the WTC "bathtub" in the late 1960s and the recent work during the recovery.

Genesis

The WTC complex consisted of seven buildings on a 16-acre site in lower Manhattan. The deep basement (bathtub) portion of the site covers a four-city block (980 foot) by two-city block (520 foot) area some 200 feet from the east shore of the Hudson River (Figure 1). The deep basement occupies only about 70 percent of the 16-acre WTC site and is just west of the place

[1] Commonly referred to as diaphragm wall construction in Europe.

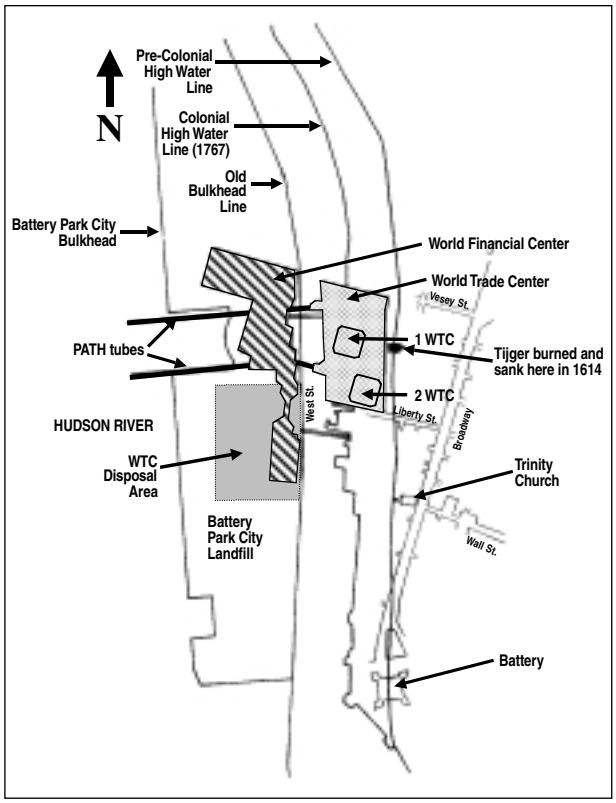

FIGURE 1 Location plan.

where the Dutch landed in 1614. The size and depth of the deep basement and the alignment of the perimeter wall were dictated by several requirements: the construction of a new interstate commuter railroad (PATH) station parallel to the Greenwich Street east wall; support for an operating New York City subway tunnel located just outside the east wall; protection of the entry points of two 100-year old, 17-foot diameter PATH tunnels on the east and west; and the foundation of the twin towers (WTC 1 and WTC 2) on bedrock within the excavation (Figure 2).

The geology of the WTC site varies from east to west. On the east (Greenwich Street), 15 to 30 feet of fill cover as much as 20 feet of glacial outwash sand and silt, below which are 5 to 20 feet of glacial till/decomposed rock. The Manhattan schist bedrock is found at depths of 65 to 80 feet. A knoll of quartzite rock intrudes into the site at the southeast corner. On the west (West Street), the fill is 20 to 35 feet thick and is underlain by 10 to 30 feet of soft organic marine clay (river mud). Below the river mud is a 20-foot thick layer of glacial outwash sand and silt and 5 to 20 feet of glacial till/decomposed rock. Bedrock is found at depths of 55 to 75 feet. Groundwater levels were within several feet of ground surface. The fills were placed into the river during various periods of development and consisted of excavation spoil, demolition debris, marine construction, abandoned vessels, lost cargo, and garbage. A maze of utilities and abandoned structures further complicated the ground conditions.

Two short segments of the West Street wall projected 65 and 90 feet to the west to permit the slurry wall to cross over the PATH tunnels where the tunnel invert was buried in rock; the top half was covered with soil. At that location, the slurry wall concrete could be cast against the top of the cast iron tunnel rings and socketed into rock on both sides of the tunnel, creating a watertight seal at the crossing (Figure 3).

The basement was bounded by a 3,500-foot long, 3-foot thick slurry wall (perimeter wall) constructed from grade and socketed into rock located at depths of as much as 80 feet. In the 1950s, continuous underground walls were constructed using bentonite slurry as a temporary support for slot excavations in difficult soil conditions. Bentonite slurry is only slightly heavier than water. Early on, the Port Authority Engineering Department recognized that this technology would be suitable for construction of a safe, economical deep basement in extremely difficult ground conditions.

The slots at the WTC were eventually filled with reinforcing steel cages that were assembled on site; each cage weighed as much as 22 tons. The cages were concreted, using Tremie methods, to form 158 individual panels. Special jointing details were used to ensure watertight connections of the individual panels that were used to form the perimeter. Each panel was approximately 22 feet long. The slurry wall was installed in a 12-month period ending in 1968.

The next phase of construction required careful staging of the excavation and temporary support of the PATH tubes that traversed the site. To provide lateral support of the wall as the excavation proceeded downward, 1,500 high-strength tendon tieback anchors were installed. Four to six tiers of tieback anchors were installed through sleeves ("trumpets") in the slurry wall, drilled through the soil using steel pipe casing, and then drilled 30 to 35 feet into bedrock. Each anchor was grouted in place, tested, and locked off at 50 percent to 100 percent of the design load. Tieback anchor capacities varied from 100 to 300 tons. About 55 additional anchors were installed to replace anchors that were obstructed during drilling, damaged during installation, or did not reach design capacity during testing.

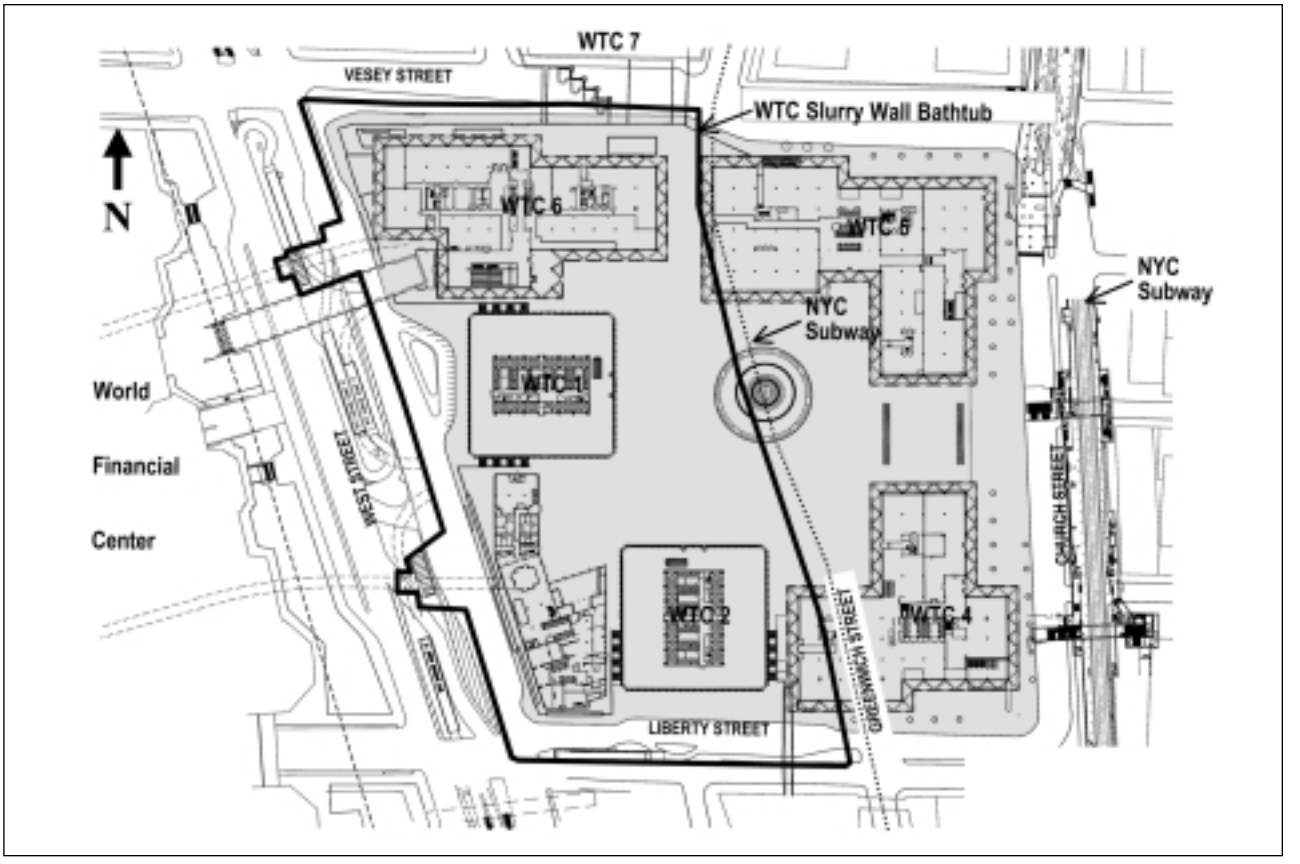

FIGURE 2 WTC site plan.

More than a million cubic yards of excavation spoil was carted to a disposal area across West Street and eventually incorporated into the landfill for Battery Park City. The southernmost building of the World Financial Center is located on that portion of the landfill (Figure 4). The excavation phase required a year. Once the permanent basement floors were capable of supporting the walls, the tieback anchors were detensioned and the sleeves sealed.

The scale of the WTC project was unprecedented. This was only the third time slurry walls were used in the United States and one of the earliest uses of a large number of tieback anchors to such high capacities. The WTC basement was the most challenging foundation construction in New York up to that time and, for that matter, up to the present (Figure 5). The Port Authority exhibited great courage and foresight when it designed and oversaw the construction of the basement structure.

Prelude

In 1993, terrorists detonated a bomb in the WTC basement adjacent to a column of the north tower (WTC 1) causing damage to the floors that were supporting the slurry walls. Fortunately, the walls themselves were not damaged, did not leak, and were able to span across the damaged areas. Visual inspection of the walls in spring 2001 revealed that the walls were in good condition.

Armageddon

On September 11, 2001, terrorists again struck the WTC complex, this time causing the collapse and destruction of the majority of above-grade structures and the partial collapse of the below-grade structures. The limits of the bathtub and the condition of the below-grade structures were not immediately evident in the aftermath of the attack.

Initial Response

Immediately after the collapse, the New York City Department of Design and Construction established a team of engineers and contractors to assist the NYC Fire Department in its search and rescue efforts. One group of engineers, under the direction of Thornton-Tomasetti Engineers (TTE), focused on the inspection of adjacent

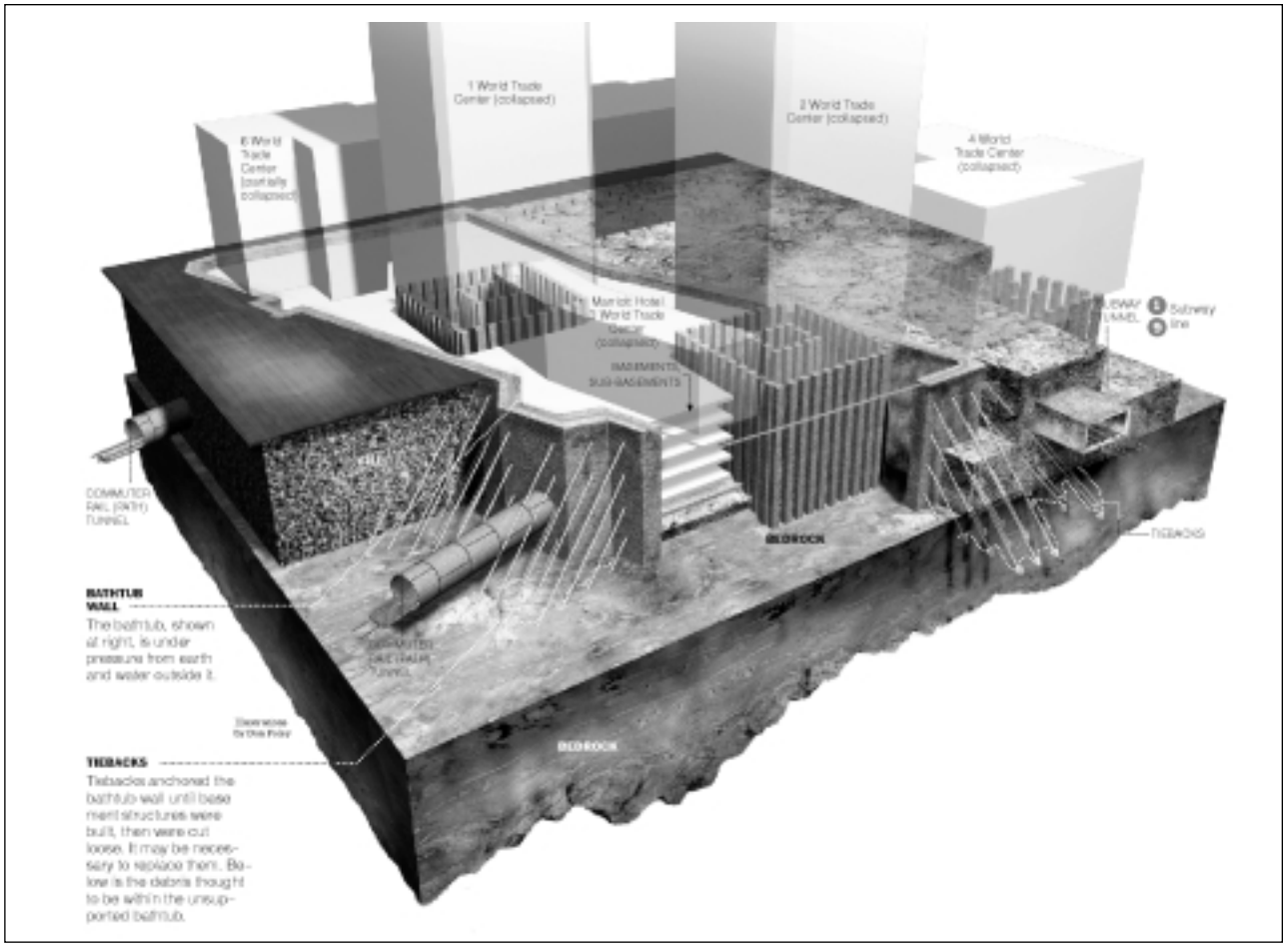

FIGURE 3 Schematic view of slurry wall/PATH crossing at West Street.

buildings while another provided advice on below-grade structures in the WTC complex, the World Financial Center complex located to the west in the Battery Park City landfill, the PATH tubes, and the New York City subway tunnels.

As heavy equipment (e.g., 1,000-ton cranes) began to arrive at the site, it became apparent that ground rules had to be established for the safe use of the equipment outside the confines of the basement, over major utilities, over access stairs to the PATH tubes and ramps, in the streets, and over structural platforms spanning open water. The use of this heavy equipment adjacent to the slurry walls or over the basement structure itself could cause the collapse of the slurry walls or any remaining basement structures. A collapse of the slurry wall would mean inundation from the nearby Hudson River.

As a first step, Mueser Rutledge Consulting Engineers (MRCE) prepared cartoon-like sketches showing the location of below-grade structures outside the slurry wall that could not be traversed by heavy equipment. The locations of four 6-foot diameter water lines were also identified. The Port Authority closed valves for two water intake lines shortly after the incident. The other two discharge water lines could backfeed river water

FIGURE 4 Original PATH tube suspension system.

into the basement during periods of high tide and had to be sealed as soon as possible. The sketches were provided to the Fire Department and the contractors for use in placing rescue, construction, and demolition equipment. Weidlinger Associates subsequently prepared more detailed utility drawings for the contractors.

PATH Tunnels

Concurrent with rescue work in New York, Port Authority engineers were investigating the condition of the PATH tunnels in Jersey City, New Jersey, where the Exchange Place Station, which was at an elevation 5 feet lower than the WTC PATH Station, had served as a sump for fire water, river water, and broken water mains discharging into the bathtub. Inspection indicated that water in the tunnels between New York and New Jersey had completely filled the north tunnel at the midriver low point. Pumps were immediately put into action to keep Exchange Place Station from flooding. As much as

FIGURE 5 Original excavation, WTC 1 steel core started, PATH tubes temporarily supported while new station is constructed along Greenwich Street slurry wall.

FIGURE 6 Current PATH tube plug at Exchange Place Station in Jersey City.

3,000 gallons per minute were pumped from the north tunnel for a 12-hour period each day. Tests of the water were inconclusive as to the source; however, most was believed to come from the vast amounts of water that were poured onto the debris to extinguish continuing fires. Within days, a 16-foot long low-strength concrete plug was placed in each tube as a seal in the event that the bathtub walls were breached and the tunnels fully flooded. The plugs were designed to withstand an 80-foot head of water pressure and will be removed once the slurry walls are fully secured (Figure 6). The Port Authority is currently preparing to remove the plugs in preparation for rehabilitation of the tunnels.

Damage Assessment

MRCE began to compile information on the condition of the slurry walls and the remaining basement structure as soon as below-grade access was possible. Teams of engineers, including MRCE, TTE, and Leslie E. Robertson Associates (LERA), and rescue personnel from FEMA, the U.S. Army Corps of Engineers, the Fire Department, and the Police Department conducted inspections of all accessible below-grade areas. These teams reported on the condition of the slurry wall, the floor slabs, and the debris fields and judged whether the floor slabs and debris could safely support the slurry walls. MRCE compiled this information on damage assessment drawings showing the locations of stable and collapsed floors, as well as the location of dense debris fields. Those diagrams were used by contractors removing the debris to prevent compromising the slurry walls; the drawings were used by MRCE in the design of the slurry wall resupport system. Figure 7 shows a typical example of a damage assessment drawing for one of the basement levels. The drawings showed that remnants of

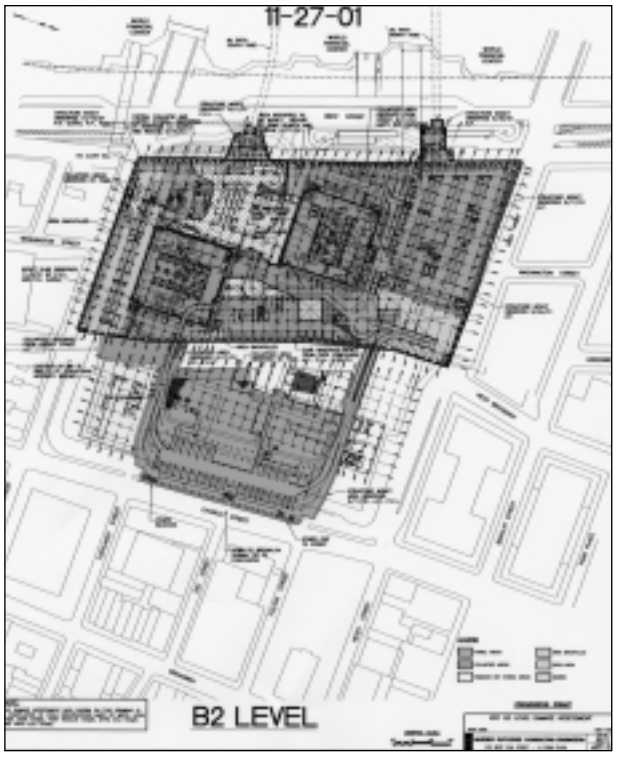

FIGURE 7 Damage assessment drawing for Level B2.

the existing floors continued to support the slurry walls in the northern sector of the site. LERA is currently reassessing the condition of the slabs in the northern sector as a temporary support for the slurry wall and for their possible reuse in a reconstructed basement.

In the center sector, the walls were supported by debris that varied from loose to compact. Along the south wall at Liberty Street, the majority of the wall was unsupported for most of its 60-foot height. Ultimately, tension cracks developed in Liberty Street immediately south of the wall, and the top of the wall moved more than 10 inches toward the site. Backfilling of the south sector began as soon as it became safe to work in the area and the extent of the problem could be determined (Figure 8). Slope inclinometers, survey points, and monitoring wells were used to measure the behavior of the wall and the groundwater levels. Dewatering wells were installed to reduce water pressure on the walls, and instrumentation was installed to measure movements. The instrumentation showed that backfilling had reduced the rate of wall movement to the point that an upper tier of tiebacks could be installed to stabilize the wall. The contractor is currently installing the fourth level of tiebacks at that location in preparation for excavation to track level by March 2002.

FIGURE 8 Backfill operations at Liberty Street.

NYC Transit Tunnels

An inspection of the subway tunnels immediately east of the slurry wall indicated that the south half of the tunnel was either collapsed or had been pierced by a falling structure (Figure 9); the north half was relatively undamaged. Bulkheads were designed at both ends to prevent inundation of an adjacent section of tunnel that was secure and operating. A more easterly subway tunnel was found to be almost undamaged and was returned to service late in October 2001. New York City Transit has prepared contract documents for reconstruction and reopening of the line by October 2002.

FIGURE 9 Damaged subway tunnel.

Resupport of Slurry Walls

The recovery of bodies, remains, and personal items, debris removal, and the excavation of residue continues under Fire Department and Police Department oversight; when human remains are discovered, work is halted to ensure their dignified removal from the site.

The abandoned "original" tieback tendons were

inspected and found to be unsuitable for reuse. Replacement anchors, intended to be permanently corrosion protected are now being installed on the south half of the bathtub; these anchors will be tested to 400 tons and locked off at 300 tons. Because of the uncertainties about the support of the wall by debris and concerns about sudden loading of the wall as a result of the collapse of the lower level floors, tieback capacity of the top two tiers of anchors was set sufficiently high so that the anchor would not fail prior to development of the ultimate moment capacity of the wall.

Tieback work is performed from inside the wall using crawler-mounted drills set on timber mats or from outside the wall using "floating leads" extending over the wall. The floating leads are used where the working surface is unsafe (Figure 10). (Excavating equipment has fallen several floors through the debris on two occasions.)

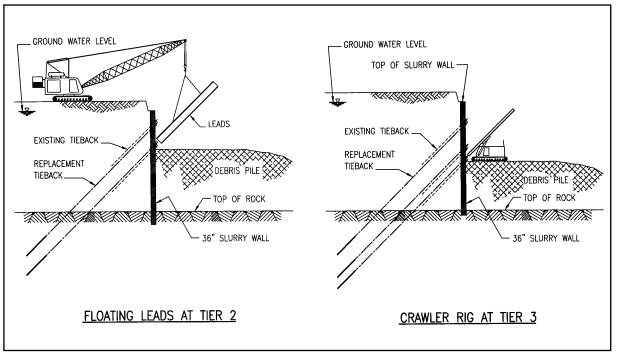

FIGURE 10 Tieback installation with floating leads and crawler rigs.

The current design requires one less tier of anchors at each wall section than was used in the original construction. At several tiers, the replacement tieback anchors will be placed either directly above or below abandoned anchors; at other tiers, the replacement anchors will be remote from abandoned original anchors. The first three tiers of anchors at the south wall were in place, and work had begun on the fourth tier as of January 2002 (Figure 11). First and second tier anchor installation on West and Greenwich Streets is proceeding from south to north as debris is removed and work space becomes available. Tiebacks will also be required

FIGURE 11 Progress along the Liberty Street slurry wall showing the installation of the fourth-tier anchors.

for a segment of the Vesey Street wall where recent demolition has caused the collapse of formerly stable floors. More than half of the first phase anchors will be in place by the end of January 2002.

As of January 2002, the slurry wall was found to be mostly intact, except for minor leaks at a few abandoned tieback seals and the upper portion of two panels at the southeast corner that were crushed by falling debris (Figure 12). The estimated time of removal of all debris is less than one year. The Port Authority has indicated its desire to restore interim PATH service in the area of the former station once the slurry walls are stabilized and the debris removal is completed. Planning for a memorial and commercial and public buildings is under way.

FIGURE 12 Damaged walls at Greenwich Street.

The events of September 11 challenged the future of our heavily engineered environment and the future of the engineering profession.

A 911 Call to the Engineering Profession

Robert Prieto is chairman of the board of Parsons Brinckerhoff, Inc.

Robert Prieto

An attack on our nation . . . thousands dead . . . 20 percent of downtown office space in Manhattan damaged or destroyed . . . more than 40 percent of the subway system capacity to lower Manhattan disrupted . . . economic costs in New York alone of $100 billion. More damage in Washington, D.C., to the symbol of our military prowess. By any measure, the events that occurred on the clear blue-sky day of September 11 were horrific. Unlike many other tragedies, all of these events were of man's own making. Unlike many past events, both natural and man-made, the events of September 11 were attacks on an "engineered," built environment, a hallmark of our society, which thrives on human proximity, connectivity, interaction, and openness. The very fabric of our "civil" society is tightly woven.

As a New Yorker who grew up and worked in the city throughout my career; as chairman of Parsons Brinckerhoff, New York's oldest engineering firm whose roots date back to 1885; and as cochair of the infrastructure task force established by the New York City Partnership in the aftermath of the attacks, I believe the 911 call of September 11 presented us with an unusual challenge, as well as an unmatched opportunity. Our response will say a great deal about the future of our heavily engineered environment (our cities), as well as about our profession. We must come to grips with necessary changes in the role of engineers and the needs of an engineered society. We must heed this call.

What lessons can we learn from the attacks of September 11 and their aftermath? What should we teach those who follow in our footsteps? How should we define "critical infrastructure" in the future? These are just a few of the questions we must answer to meet history's challenge. We must return to the age-old fundamentals of education, namely the 3Rs. But in the highly engineered environment of the twenty-first century, the traditional 3Rs of reading, 'riting and 'rithmetic have been replaced by *resistance*, *response*, and *recovery*.

Critical infrastructure must be designed to *resist* attack and catastrophic failure. Immediately after the attacks and the subsequent collapse of the World Trade Center towers, some of the pundits suggested that high-profile buildings and other critical infrastructure be designed to stop airplanes. Simply put, this is utter nonsense, a disservice to our profession and to society in general. Unless we are prepared to live in an engineered environment that resembles the complex of caves in Afghanistan, we will not design buildings to stop planes. The challenge is to keep airplanes away from buildings and to root out those who challenge our way of life at the source. We must resist the urge to overreact in the short term.

But that does not mean we should not make changes. Every engineering disaster, whether natural or man-made, teaches us something. Sometimes the lessons that lead to a deeper understanding of the real challenges we face are only disseminated to a subset of our profession. Because our profession tends toward specialization, we often have difficulty translating lessons learned to a broad range of disciplines and industry segments. Here is where the NAE could play an important role. The academy could gather information on everything being done, draw lessons from an incident, consolidate this knowledge, and ensure that it is distributed to a wide range of disciplines and industries.

In New York on September 11, we saw the best of engineering, not the failure of engineering. We saw two proud structures swallow two, maliciously guided planes, fully loaded with fuel. The structures not only endured impacts beyond their design basis, but also withstood the ensuing fires; they were not immediately overwhelmed. The buildings were the first of the many heroes that died that day, but only after they had remained standing long enough for as many as 25,000 people to escape. This is the true testament to the designers. In Washington, D.C., we also saw the best of engineering. The Pentagon's resistance to a large-scale, direct, deliberate assault speaks well of our ability to design critical infrastructure to resist attacks. The successful resistance of the towers and the Pentagon in no way diminishes the human tragedy of that awful day.

As we move forward, we must learn what we can from these tragedies and, as we have in the past, we must incorporate these lessons into future designs. With a comprehensive understanding and broad distribution of these lessons, we can begin to address the larger consequences of the disaster. Not all of the damage was incurred by high-profile buildings in New York and Washington. Damage to surrounding infrastructure—transportation, electricity, and telephone—exceeded (in economic terms) the damage to the buildings. The very purpose of infrastructure—to tie development together—in some ways limits its ability to resist deliberate attack.

The 3 Rs for the twenty-first century are resistance, response, and recovery.

The second "R" is *response*. The attacks left large portions of the transportation, electricity, and telephone networks that service lower Manhattan inoperable and compromised the entire system. In the immediate aftermath of the attacks, transit system operators modified system operation to stop passenger flow into the affected area and remove trains that were already in the area. Their timely actions prevented loss of life to transit passengers and workers, despite the subsequent destruction from falling debris. But then came an even more daunting challenge—to reconfigure the transportation system to meet the needs of the 850 businesses and 125,000 workers who were physically displaced when 25 million square feet of office space was damaged or destroyed and to provide service to the more than 350,000 passengers to lower Manhattan whose commuting patterns were disrupted. Herein lie some of the most valuable lessons for our highly engineered environments.

The first major lesson of September 11 is that *infrastructure and development are intricately linked.* Although infrastructure is the *sine qua non* of development and vice versa, we rarely appreciate their interdependencies

until we must respond to a new paradigm, such as the aftermath of September 11. Along with the "localized" failure of "development" (the collapse of the World Trade Center towers), there was localized failure of the attendant infrastructures (e.g., a subway line, the local power grid, the PATH station at the World Trade Center, etc.). In response, we reconfigured regional development (an estimated 29,000 employees working outside of New York City and another 29,000 temporarily working out of other space in the city). We also reconfigured our regional transportation network (e.g., mandatory HOV into the city, increased ferry service, increased transit ridership at other river crossings, etc.). Analogous steps were taken for the utility and telecommunications networks

The second lesson of September 11 is that the *core capacity of infrastructure systems is essential*. By "core capacity" I mean the degree of interconnectivity of the elements of a system, as well as the number of alternative paths available (i.e., a system's flexibility and redundancy). Sometime before September 11, I attempted to explain the importance of some planned improvements to our transportation system to government officials. I explained that these improvements would enhance the core capacity of a well developed transportation network and would improve overall system reliability, availability, and performance. The benefits of these additions to core capacity would strengthen the overall system and would go well beyond the benefits of adding a new system connection from point A to point B. Unfortunately, my argument for strengthening a complex system in the most complex, engineered urban environment in the world was largely lost. Traditional project evaluation models have focused on the "value" of new connections, ignoring their broader system-wide implications. Improved reliability, availability, and performance from added core capacity to a complex system can pay dividends that are not always apparent.

In large measure, the capability of responding to September 11 was the result of good, timely maintenance.

My argument for improving regional transit systems proved itself in the aftermath of September 11. The core capacity of the affected systems provided the flexibility for dealing with commuting patterns that had to be modified overnight (literally); lines and stations outside the immediately affected area were able to handle passenger volumes exceeding those that a point A to B connection would have achieved. Several days after the attacks, I was gratified to receive a call from these same government officials who now understood the importance of core capacity.

The infrastructure systems impacted by September 11 responded more or less quickly depending on their core capacities and the concentration of critical infrastructure in the damaged area. Older, more mature systems responded better than many newer systems, which were still heavily focused on building new connections and did not yet have as high a level of core capacity. This experience suggests that core capacity should be a criterion in the planning and implementation stages of new infrastructure.

Core capacity is not just the extent of a system or the number of alternative system paths. It is also the intrinsic quality of the system when it comes under stress. This brings us to the third lesson of September 11—*deferred maintenance represents a real cost and a real risk*.

The history of engineering is marked by exciting breakthroughs, great works of master builders, and outstanding service. Regretfully, it is also marked by the systemic degradation of some of our greatest achievements. Society at large, and even some people in the engineering profession, do not consider sustained maintenance as important as the creation of new projects. For many reasons, we have allowed some of our most complex systems to fall into disrepair thus compromising their level of reliability, availability, and safety. The problem is most apparent in failing rail systems in England and the United States, but deferred maintenance affects every element of infrastructure.

Not too long ago, the New York City transit system was in urgent need of repair and maintenance. Out of that crisis emerged a commitment to fund, reorganize, rebuild, improve, and maintain the system to a well-defined standard. To a large measure, the capability of responding to September 11 was the result of good, timely maintenance. Other elements of infrastructure with higher backlogs of deferred maintenance are struggling to keep up.

The fourth lesson of September 11 is that *operational and emergency response training is an integral element of critical infrastructure response*. Just as we factor constructability reviews into our design process and maintainability considerations into our construction details, we must include operational training in our engineering of critical infrastructure. The many areas of exceptional performance in response to September 11 underscores the point. The events also revealed the need for new scenarios. We must be prepared to respond to new threats in the form of weapons of mass destruction, higher risks of collateral physical and economic damage, and more extended response times. Training of first responders must be integrated with operational training for infrastructure systems. We must also understand how first responder teams have evolved with our increasingly engineered environment.

The fifth lesson of September 11 is that *the first responder team must include engineers and builders in addition to the traditional triad of fire, police, and emergency services*. On September 11, the engineering and construction industry voluntarily reached out to provide technical and construction expertise. Although protocols were not firmly in place and this "fourth responder" had not participated in response training, the help of engineers and constructors has been critical.

From now on, response protocols in engineered urban environments must incorporate this "fourth responder," and dedicated training facilities must reflect the unique nature of highly engineered environments and their infrastructures. Legislation must also be passed to remove the risks that accrue to engineer "volunteers" who are not covered by Good Samaritan statutes.

The third "R" is *recovery*. Building in as much resistance as makes sense from a risk-weighted, operational, and economic perspective enhances our ability to respond. We can provide core capacity, focus on reliability, availability, and performance, and reconfigure inherently resilient systems. But we must also plan for the recovery of the capacity and service that was destroyed. We must be prepared to restore the engineered fabric, making it even better than it was. In other words, we must engineer critical infrastructure for recovery in the following ways:

- ensuring accessibility to the sites of critical infrastructure
- ensuring the availability of specialized construction equipment, contracts, and materials
- developing a well documented system with clear interface points
- preplanning and rehearsing response and recovery scenarios for high-probability events (e.g., earthquakes, hurricanes, floods)

But, to truly respond, even more will be needed—an effective response also requires a *vision*. Every aspect of the engineered environment must be understood not only in terms of its past and present, but perhaps more importantly, in terms of its future—how it will evolve; how resistance, response, and recovery can be built into the system as it expands; how it fits into the vision of the future; and what role it plays in the overall engineered environment. Effective recovery can only begin with this vision.

On September 11, the engineering and construction industry voluntarily reached out to provide technical expertise.

The 3Rs—resistance, response, and recovery—can provide a new framework for engineering our critical infrastructure in the aftermath of September 11. But we must prioritize our efforts in terms of our most critical needs. To put it simply, we must agree on what comprises critical infrastructure. Here, I confess my own predisposition to adopt a broad view of system behavior. In those terms, we can identify the following characteristics of critical infrastructure systems:

- Rapid failure would lead to a catastrophic loss of life (by rapid I mean relative to the consequences possible as opposed to an absolute time scale).
- Failure or significant degradation would have unacceptable economic consequences.
- Rapid failure would significantly undermine rescue and response efforts (e.g., if emergency operations centers were located in proximity to high-profile targets).

- Significant degradation would significantly interfere with recovery efforts.

Engineers must become the master builders of the twenty-first century. We must be systems thinkers, determined visionaries, and political pragmatists imbued with the ethics and integrity that have made engineering a proud profession. Engineers must design for the 3Rs, as well as for functionality, safety, reliability, maintainability, and sustainability. We cannot be content to play a secondary role in building our future. We must have a voice, and we must take risks. In short, we must be leaders!

We need a planning process—rather than a static plan—to protect our homeland.

Homeland Security: Building a National Strategy

Ruth David, a newly elected member of the NAE, is president and CEO of ANSER, Inc., which includes the ANSER Institute for Homeland Security.

Ruth David

On September 11, 2001, our nation was stunned by the sheer audacity of the al Qaeda terrorists. The devastation—human lives lost and symbols of our free society destroyed—left an indelible mark on the American psyche. In the aftermath we are left to rebuild our sense of personal safety and national security even as we wage war against terrorism on a global scale.

Although we were rightly horrified by the attacks, we should not have been surprised by the aggression. Osama bin Laden himself provided ample warning; in a January 1999 interview, for example, he said "hostility toward America is a religious duty, and we hope to be rewarded for it by God . . . . I am confident that Muslims will be able to end the legend of the so-called superpower that is America." This was not empty rhetoric; bin Laden was implicated in the 1993 attack on the World Trade Center, the 1996 Khobar Towers bombing, the 1998 American embassy bombings in Africa, and the 2000 bombing of the *USS Cole*. So—having been warned—why were we unprepared?

Before September 11

For the past decade, a steady parade of studies, task forces, and commissions have expressed growing concerns about threats to the American homeland. The 1997 National Defense Panel described adversaries who were willing to confront us at home—as well as abroad—using asymmetric techniques to

counter our traditional military strengths. The panel also noted the growing importance of homeland defense as an element of national security (National Defense Panel, 1997). In 1999, the United States Commission on National Security/21st Century was asked to help create a national security strategy appropriate to the emerging threat environment. In the commission's Phase I report, published in September 1999, the number one conclusion was that "America will become increasingly vulnerable to hostile attack on our homeland, and our military superiority will not entirely protect us" (USCNS, 1999). The final report, published in January 2001, predicted that "a direct attack against American citizens *on American soil* is likely over the next quarter century" (USCNS, 2001). None of these reports, however, conveyed a sense of immediacy—in spite of evidence to the contrary.

On September 11, 2001, "homeland security" had still not been defined.

I do not mean to suggest that we completely ignored the asymmetric threat. However, the lack of urgency and the absence of a strategy limited our progress toward the redefinition and transformation of our national security apparatus. Although our military capabilities have improved significantly in the past few decades, our forces have remained optimized for traditional warfighting—on a foreign battlefield—against a known enemy. The mountain of reports describing the asymmetric threat from various perspectives offered piecemeal, and often conflicting, solutions. When confronted with new demands, organizations that were overcommitted already inevitably called for new resources. A plethora of working groups and task forces were established solely to bridge the fault lines between agencies. The national security lexicon expanded to include new terms, such as weapons of mass destruction, weapons of mass effect, chemical/biological/radiological/nuclear/explosive, cyberterrorism, and critical infrastructures. But after nearly a decade of debate, protecting our homeland from asymmetric threats was still not a primary mission for any part of our government. On September 11, 2001, *homeland security* had still not been defined. In short, there was a great deal of activity but little progress toward resolving the core issues, which will necessarily impinge on legacy missions—and bureaucratic turf.

The Aftermath

September 11 provided a wake-up call to our nation. Suddenly the debate about *if versus when* there might be a catastrophic attack on our homeland was transformed to *where next*. The subsequent anthrax attacks made the threat of biological warfare real to the American public and strengthened our collective resolve. Even as the ruins of the World Trade Center continued to smolder, we mobilized our military to wage war against global terrorism.

At the same time, homeland security—still undefined—jumped to the top of the priority list for every branch of the federal government, many state and local governments, and even parts of private industry. On October 8, 2001, the President issued an Executive Order establishing the Office of Homeland Security with the mission "to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks." In the Quadrennial Defense Review Report released on September 30, the U.S. Department of Defense "restored defense of the United States as its primary mission," even as U.S. forces went on the offensive against global terrorism (DOD, 2001). The Federal Aviation Administration took immediate action to strengthen airport security. The Federal Bureau of Investigation restructured its headquarters to increase its focus on the *prevention*—rather than the *investigation*—of terrorist attacks. The anthrax attacks provided an additional impetus to the nascent bioterrorism program in the U.S. Department of Health and Human Services and heightened concerns in the U.S. Department of Agriculture. Organizations with the words "homeland security" in their titles suddenly cropped up throughout government and industry. Legislation was introduced, and budgets were augmented—all before we had developed a strategy or defined our priorities.

If we fast-forward to the first anniversary of our wake-up call, it is easy to imagine two potential—and equally undesirable—outcomes. Given the vast number of vulnerabilities inherent to our free society, and given the absence of clearly established national priorities, we could easily spend billions of taxpayer dollars and make

little meaningful progress toward protecting our homeland from future terrorist threats or attacks. Alternatively, if Osama bin Laden fades from the scene and we experience no additional catastrophic attacks, we could declare success, turn our attention to other national issues, and continue to let entrenched bureaucracies prevail—thus allowing the current patchwork of organizational strategies to substitute for a national strategy.

To avoid these mistakes, we should learn from the past. After winning the Cold War, we failed to retool our national security establishment for the emerging asymmetric threat environment even though the need was discussed ad nauseam. In the aftermath of September 11, we heard the usual calls to investigate the organizational failures that had *permitted* the attacks. Instead of looking for culprits, we should consider it a failure of national strategy, policy, and will. The bottom line is that we—collectively—failed to heed well documented concerns; we did not make the tough decisions necessary to defend our homeland effectively. We should not assume that Osama bin Laden and his al Qaeda network are the only ones with the ability or desire to use asymmetric weapons; history is replete with examples. Nor should we assume that large oceans and friendly neighbors, even when backed by military power, can provide sanctuary from asymmetric threats. September 11 should be example enough. To protect our nation we must also defend our homeland.

Planning

Developing a strategy will be hard—and implementing it will be even harder. A national strategy for ensuring the security of our homeland will engage players who have not been part of our traditional national security apparatus—such as Health and Human Services and the Department of Agriculture. The strategy must bridge the gap between *foreign* intelligence and *domestic* intelligence authorities and policies—recognizing that geographic boundaries are not absolute in an era of global markets and coalition warfare. Federal control will have to be ceded to exploit inherently distributed authorities—as well as to leverage the knowledge and resources of other stakeholders. A comprehensive national strategy must link federal, state, and local strategies and integrate the strategies of private corporations who own much of our nation's critical infrastructure. It should include an education and training program that supports the adaptation of operational strategy as well as tactical preparedness in a world of evolving threats and thinking enemies. It must provide a strategy for communication so we can share information—what we know and what we don't know—with American citizens as well as operational communities. A national strategy will be supported—*but not replaced*—by a comprehensive budget plan that aligns resources with national priorities. An effective strategy for homeland security will inevitably alter the missions of many existing organizations—and most likely will require the creation of new organizations with new missions. Building such a strategy will be hard—but we must do it. We can no longer afford either the lowest common denominator solution that too often emerges from fully coordinated efforts or the patchwork of point solutions contributed by individual agencies.

Perhaps the greatest initial challenge will be defining success. What is the ultimate goal of the homeland security mission? How will we define success? Are we defending America—the nation—or protecting every individual American from every conceivable terrorist threat? If we set the bar too high, the resource requirements will be unaffordable and the loss of personal freedoms untenable. If we set it too low, American citizens may lose confidence in the government's ability to protect the nation from terrorism. If we fail to answer the question, we will have no context for making decisions.

Federal control will have to be ceded to exploit inherently distributed authority and to leverage the knowledge and resources of other stakeholders.

Once we have defined success, we must identify interim outcomes against which progress can be measured. This will require that we define priorities against which resources can be allocated, as well as responsibilities against which performance can be evaluated. These are the basics of any good strategy. But a definition in the context of homeland security presents a formidable challenge because of the scope of our national objectives, the

diversity of the potential threats, and the fragmented ownership of both resources and responsibilities.

Strategic Framework

Ensuring the security of our homeland is inherently a multidimensional problem. A relatively simple framework would include three dimensions—national objectives, potential threats against which we are defending, and the operational entities that will implement the strategies.

A comprehensive strategy for homeland security must encompass all phases of the strategic cycle. Therefore, the national objectives must be *deterrence, prevention, preemption, crisis management, consequence management, attribution,* and *response* (ANSER, 2001). The ultimate goal, of course, is to *deter* future attacks—by convincing the enemy that their efforts will be unsuccessful and/or that our response will be both immediate and devastating. But our traditional deterrence model is inadequate in a world in which suicide missions are common, commercial objects can be used as weapons, attacks can be launched anonymously, and adversaries may occupy no sovereign territory that can be held at risk. Therefore, although maintaining our nuclear and conventional military power is vital to our nation's security, we must also bolster our security with a national policy and defense capabilities that explicitly address asymmetric threats to our homeland. In short, this will mean we must implement strategies to *prevent* the acquisition or delivery of asymmetric weapons, to *preempt* attacks already in motion, to limit the impact of an attack through *crisis* and *consequence management,* to *attribute* an attack to the perpetrator as well as the ultimate sponsor, and to *respond* immediately with the full force of our military and/or legal establishments. Deterrence will be most effective if our intent is made clear through policy and our ability is underpinned by operational capabilities that address all phases of the strategic cycle.

We must protect our homeland, but we must also protect the strengths of our nation.

The spectrum of asymmetric options includes biological, chemical, unconventional nuclear or radiological, cyber, and enhanced conventional weapons—and is limited only by our adversaries' imaginations (ANSER, 2001). We cannot hope to protect every building from a truck bomb or every public event from a biological release; nor can we afford to inspect every item that crosses our borders. For some threats, our focus will necessarily be on the latter part of the strategic cycle—dealing with the aftermath. We must, however, think through the spectrum of possibilities and make conscious decisions about the defenses we will implement, as well as how we can improve our capability of mitigating the impact of a catastrophic attack. And our ability to attribute an attack, coupled with the will to respond, must be apparent.

The strength of our nation is based on the distribution of authority and power among federal, state, and local governments, the free market that is the basis of our economy, and the personal freedom and privacy afforded to every citizen. Responsibility for protecting our homeland is distributed across a range of diverse organizations—complicating the development and implementation of a national strategy. How can we ensure that related fragments of information are fused to create national—versus local—situational awareness? How can we create the excess capacity that would be needed to respond to a biological attack in a market-driven health care system? How can we identify terrorists living among us without infringing on the privacy of our citizens? We must defend our homeland, but we must also protect the strengths of our nation.

The goal should be a national strategy—*not a federal strategy*—a synergy of the actions of individual organizations at all levels, ensuring that gaps are filled, conflicts are eliminated, and overlaps are minimized. The three-dimensional framework in Figure 1 may help to visualize the inherent complexities of the challenge. Within each subcube, we have a national objective, a threat category, and operational entities with varying responsibilities. Although operational responsibilities will not be uniformly distributed, a comprehensive national strategy must assign missions and authorities within each space.

Implementation

If we try populating the framework with current organizations and assigned missions, we can get an idea of

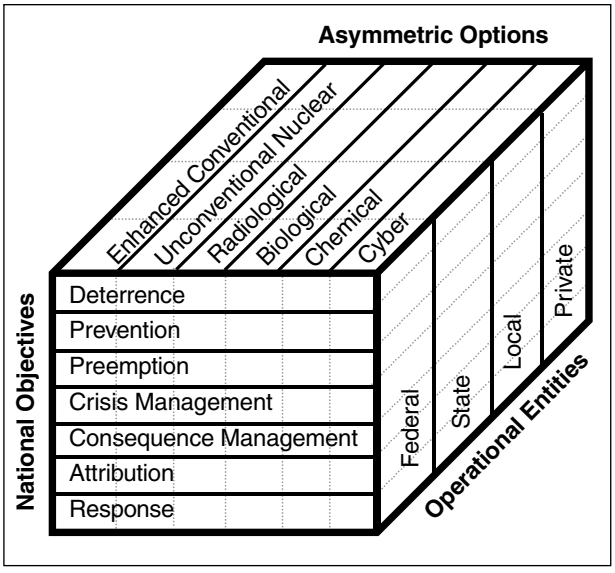

FIGURE 1 Strategic framework for homeland security.

the lack of coherence in our current state. Fault lines created by legacy missions appear not only at subcube boundaries, but also within each space. We cannot effectively define a strategy for meeting one national objective in isolation any more than a single organization can define its strategies in isolation.

The strategic cycle is a continuum rather than a set of discrete objectives, and success will depend on the sharing of information around the entire cycle. At any given time, we will be working to deter and prevent future attacks on our homeland; the insights gained will provide useful information for the consequence management community as it prepares for potential future attacks. Knowledge acquired through a preempted attack may inform national response and help deter future attempts. In other words, the boundaries between foreign and domestic intelligence authorities, as well as between national security and homeland security, will create additional fault lines that must be bridged.

Each threat category introduces its own complexities for various parts of the strategic cycle. It will be difficult to prevent an adversary from acquiring or delivering an asymmetric weapon—particularly when the weapon can be constructed from commercially available components and our own infrastructure can serve as a delivery system. Prior to September 11, few people would have included commercial airliners on the list of asymmetric weapons; even fewer would have called our U.S. Postal Service a weapon delivery system. In some instances, particularly if we are talking about biological or cyber weapons, it may be difficult to detect an attack. Cyberterrorists can hide their preparations in a background of hacker noise, can operate from safe havens far from the point of attack, and can choose from a variety of failure modes—some of which may be indistinguishable from common system failures. The slow-motion aspect of bioattacks, coupled with their similarity to natural outbreaks of disease, will complicate early detection and, therefore, our ability to mitigate the consequences—as well as to ensure positive attribution. Crisis and consequence management strategies designed for an explosion cannot equip us to deal with a biological attack. We must analyze each threat category separately across the full range of objectives to identify situations that require unique capabilities.

To build effective defenses, and to ensure our ability to mitigate the impact in case of an attack, will require that we identify likely targets for each threat category. Potential homeland targets include large gatherings of people, symbolic facilities, and critical information or infrastructures—including industries that underpin our national economy. It is readily apparent that the possibilities are endless—and equally apparent that we cannot hope to imagine every potential attack. But too often we focus our resources on preventing a recurrence of the last attack rather than imagining the next one. Recent terrorist attacks—and attempted attacks—demonstrated significant creativity on the part of our adversaries; but our nation's capacity for innovation can provide a formidable basis for the development and evolution of a national strategy. What we need is an ongoing process that includes imagining attack scenarios, drafting strategies that span the cycle of national objectives, and independent gaming to test the efficacy of strategies. Over time, this approach will yield increasingly robust national strategies; the challenge will be to create new scenarios continually to keep us one step ahead of our adversaries, who will be observing us and learning from our actions.

But even the best strategy will be worthless unless it is implemented. Therefore, we must also develop a national playbook—a living playbook—to guide the activities of diverse operational entities. Just as no sports team can be fielded without practicing, our homeland security teams must participate in exercises to build relationships and institutionalize processes, thereby creating an end-to-end capability. In the aftermath of the September 11 attacks, it became clear that some federal

authorities, some local authorities, and some private companies all had fragments of information related to the attacks; but we had neither processes nor relationships in place to construct an operational picture until it was too late. The same thing could happen if a biological attack were launched against us. Our nation has never confronted a deliberately introduced contagious pathogen, but we know that a biological warfare attack is unlikely to obey traditional public health models that predict the spread of infectious disease. Therefore, our ability to mitigate the consequences of such an attack will depend in large measure on our having exercised in advance contingency plans to keep our society functioning. Plans and exercises cannot cover every possible attack, but they will, over time, create a robust capability for protecting our homeland.

The question that continues to plague the government is *who is in charge*. The answer must be—*it depends*. Even at the federal level, there is no way to reorganize so that a single individual—apart from the President—would be in charge for every conceivable situation. In addition, much of the responsibility for homeland security will be vested in organizations outside the federal government. We must not let our desire for hierarchical command and control become our Achilles heel. Through ongoing scenario development, planning, and exercises, we can, over time, find an answer to the question. But it is likely to be *it depends*.

Conclusion

We have never lived in a risk-free world—and a comprehensive national strategy for homeland security will not change that. We must aim for success—deterrence of future terrorist attacks—but prepare for failure. We must build strategies for each phase of the strategic cycle to meet a broad spectrum of potential threats. These strategies must define people, processes, and technologies—in military terms, training, doctrine, and materiel—and must clearly assign responsibility and accountability to appropriate operational entities. The strategies must be accompanied by measurable outcomes and clear metrics and must be supported by a comprehensive budget plan that aligns resources with responsibilities.

But we must not stop there. We are facing a world in which agility defeats bureaucracy. We need a planning process—rather than a static plan—to protect our homeland. Only by continually adapting our plans to new threat scenarios and exercising those plans can we hope to defend ourselves against evolving threats and thinking enemies. As Dwight Eisenhower aptly said, "In preparing for battle I have always found that plans are useless, but planning is indispensable."

References

ANSER. 2001. A Primer on Homeland Security: Strategic Functions, Threats, and Mission Areas, by Randy Larsen and Dave McIntyre. Available online at: <*http://www.homelandsecurity.org*>.

DOD (U.S. Department of Defense). 2001. Quadrennial Defense Review Report. Washington, D.C.: U.S. Department of Defense.

National Defense Panel. 1997. Transforming Defense: National Security in the 21st Century. Washington, D.C.: U.S. Department of Defense.

USCNS (United States Commission on National Security/21st Century). 1999. New World Coming: American Security in the 21st Century. Available online at: <*www.nssg.gov*>.

USCNS. 2001. Road Map for National Security: Imperative for Change. Available online at: <*www.nssg.gov*>.

Policy makers and scientists must assess the probability of threats as well as the amount of damage they might do.

Bioterrorism: Threat and Preparedness

Michael J. Powers and Jonathan Ban

Michael J. Powers

Jonathan Ban

Prior to the anthrax mailings that followed the terrorist attacks of September 11, much of the criticism about planning and preparedness for bioterrorism attacks had been focused on the mismatch between the assessments of the threat and the size and structure of the planned response. Many analysts had criticized plans for overemphasizing worst-case scenarios and underemphasizing more probable middle- and low-casualty attacks. Most worst-case scenarios involved the release of a military-style biological agent in aerosol form near an urban center; everyone exposed to the pathogen would become severely ill, and many would die; casualties would number in the tens or even hundreds of thousands. Scenarios involving contagious pathogens, such as smallpox or plague, were even more worrisome. Outbreaks involving such pathogens evolve over time, and unless appropriate measures are taken, the numbers infected and the size of the affected geographic area would expand exponentially.

The anthrax mailings were not the mass-casualty bioterrorism many had expected. Although the military-grade anthrax agent was highly sophisticated, it was delivered in a relatively unsophisticated way—through the mail system. As a result, there were relatively small, localized incidents that led

Michael J. Powers and Jonathan Ban are research associates at the Chemical and Biological Arms Institute in Washington, D.C.

to a limited number of illnesses and deaths. The incidents aroused significant fear and disruptions but not mass casualties. Based on these attacks, some analysts have suggested that terrorists would not be able to orchestrate mass-casualty attacks using biological weapons. Others have considered these attacks as demonstrations of terrorists' ability to acquire high-quality anthrax, thus crossing an important threshold. Because those responsible for the mailings did acquire (whether they also manufactured the agent remains unclear) high-grade anthrax agent but did not disseminate a sufficient quantity to produce mass casualties, both arguments are correct.

Assessments of bioterrorist threats have either been unfocused or narrowly focused on single factors.

The anthrax mailings brought to public attention a recurring problem in national security planning: expectations of future developments are often vastly different from what actually occurs. Therefore, rather than planning for a narrow range of least-likely, high-consequence contingencies or focusing only on additional mailborne anthrax attacks, we must plan for a variety of future incidents—including incidents that cause mass casualties and mass disruption. In fact, planning for a variety of more likely, middle- to low-casualty incidents, while simultaneously being prepared for low-probability, high-consequence incidents is perhaps the most significant challenge facing planners. The cornerstone of preparations for future bioterrorist incidents, regardless of their nature or scope, must be a national, but not necessarily federal, public health system capable of detecting, assessing, and responding to a broad variety of contingencies.

The Challenge

Assessments of the bioterrorist threat are often either unfocused or narrowly focused on single factors. The mismatch between threat assessments and preparedness efforts can be explained partly by the failure of threat assessment methodologies to take into account all of the factors comprising the threat. Single-factor threat assessments, for example, focus either on the terrorists' motivations and objectives or on the hypothetical effects of a biological weapon, but they do not indicate which scenarios are plausible or their comparative likelihood. Consider, for example, a terrorist attack involving smallpox, which is often cited as the worst-case scenario for several reasons. First, smallpox is a highly contagious disease. Second, the population has little or no immunity to the disease. Third, even with large stockpiles of smallpox vaccine, given our highly mobile life style, it would be difficult to contain an outbreak.

We must, however, keep this threat in perspective. Despite the catastrophic effects of a smallpox attack, the probability of such an attack is extremely low, especially compared to the probability of other scenarios. First, smallpox as a naturally occurring disease has been eradicated. Second, the virus that causes smallpox is known to exist in only two high-security laboratories—one in Atlanta at the Centers for Disease Control and one at the Vector Laboratories in Siberia, Russia. Therefore, it would be extremely difficult for a terrorist to acquire the smallpox virus. Moreover, the effects of a smallpox attack would be uncontrollable and, therefore, could also affect the terrorists and their supporting constituencies. If we look at all of these factors, we must conclude that a smallpox attack is a *potential* contingency, even, perhaps, the most damaging potential contingency, but the *probability* of occurrence is very low. Nevertheless, smallpox has received the lion's share of attention and has drawn attention away from the wide range of other agents that could be used.

Rather than focusing on vulnerability to a particular organism or looking to history to determine what is to come, policy makers and scientists must recognize that the bioterrorist threat is not unidimensional. We must consider four key elements of the threat: the *who* (the actor), the *what* (the agent), the *where* (the target), and the *how* (the mode of attack). The impact of a bioterrorist attack will be determined by the interaction of these components. The more casualties bioterrorists seek to inflict, the more difficult it will be for them to assemble the necessary combination of these components. Thus, the level of risk declines as the level of desired casualties increases because the attack scenario *becomes less likely*.

For a number of reasons, including technical difficulties and the absence of motivation, a catastrophic

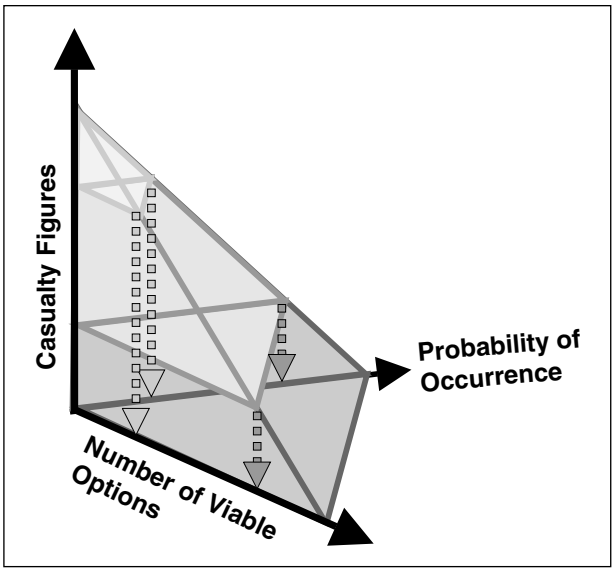

FIGURE 1 Assessing the bioterrorist threat.

bioterrorist event is not the most likely contingency. Only the release of a very contagious or very high-quality agent by a highly efficient dissemination technique could result in thousands or more casualties. In reality, the number of pathways open to terrorists that would result in catastrophic numbers of casualties are few, and those that do exist are technically difficult. The number of technical pathways for producing a low- to mid-range bioterrorism incident are more numerous, less technically challenging, and more suited to the motivations and constraints of traditional concepts of terrorism. Figure 1 is a graphic representation of the bioterrorism "threat envelope." As the pyramid illustrates, the higher one moves on the casualty axis, the lower the probability of occurrence and the number of viable options. Thus, the terrorist is left with relatively few, and very challenging, contingencies for inflicting mass casualties.

Despite the low probability of a catastrophic bioterrorist attack, there is still ample cause for concern. We do not know how "massive" an attack would have to be to overwhelm the response system, instill fear and panic, or cause serious political or economic fallout. Although many terrorists will not be interested in using biological weapons or will not be able to do so, two categories of nonstate actors—those with relationships with national governments and those outside the traditional scope of governmental scrutiny—warrant particular attention. The uncertainties surrounding bioterrorism will remain, and although terrorists have yet to demonstrate the sophistication required to carry out large-scale attacks with biological weapons, the World Trade Center and Pentagon attacks have shown a willingness to inflict mass casualties. Meanwhile, the rapid development of biotechnology and the diffusion of expertise in this field may lower the technical bar over time.

Preparedness

To date, the driving factor in planning and preparedness has been meeting the threat of catastrophic casualties, without regard for its low probability. However, in our view, the relationship between the probability of occurrence and the consequences should be the basis for setting policy. Because financial resources are finite, policy makers will have to make difficult choices. Should the focus be on promoting preparedness for a single biological agent, or should we invest in measures that promote preparedness for a variety of agents and scenarios? Every dollar spent preparing for a specific agent, such as building stocks of smallpox or anthrax vaccine or purchasing antidote for botulinum toxin, is a dollar that cannot be spent on preparedness for other organisms. Given the variety of combinations among actors, agents, targets, and dissemination techniques, a public health system must be capable of rapidly and accurately detecting and assessing a large number of bioterrorism scenarios and addressing most contingencies. Rather than limiting planning and preparedness to a narrow range of catastrophic scenarios, planning should be based on developing the capability of effectively and efficiently responding to a variety of bioterrorist contingencies. In our judgment, the emphasis should be on building capacity in the public health system.

Many people assume that preparing for high-end attacks will also provide a capability of responding to middle- and low-range attacks. Consider, for example, the contents of the national pharmaceutical stockpile. In the wake of the recent anthrax attacks, the Centers for Disease Control plans to expand the national pharmaceutical stockpile and accelerate the procurement of vaccines. The bioterrorism preparedness budget currently being debated in Congress includes approximately $509 million for the procurement of smallpox vaccine, enough to vaccinate nearly every U.S. citizen. Although focusing on such high-end attack scenarios simplifies planning and preparedness by narrowing the range of contingencies, it also introduces a substantial degree of risk that the public health and medical system will be unprepared for more likely, but less drastic contingencies. Furthermore, smallpox vaccine is useless

against all other agents, including anthrax, botulinum toxin, tularemia, and brucellosis. Therefore, we run the risk of neglecting other measures that could be used to meet a wide range of contingencies. We must strike a better balance between hedging our defenses against high-end, mass-casualty events and building a "system of systems" capable of addressing both a wider range of bioterrorist contingencies and natural outbreaks of infectious disease.

A national surveillance system to provide an early warning of outbreaks of disease will be critical to our preparedness.

A System of Systems

There is no silver bullet to meet the bioterrorist challenge. Preparedness cannot be focused on a single tool for addressing the problem but must be on a system of systems that integrates a broad range of activities. The nation's public health resources—surveillance systems, epidemiological expertise, and laboratory networks—must be integrated with health care, emergency management, law enforcement systems, and others, and all of these must be connected by a system for sharing information and communicating across sectors.

Bioterrorism differs from other types of mass-casualty terrorism (e.g., chemical, radiological, or nuclear terrorism) in that it would impose heavy demands on the public health and health care systems, which would be called upon to mitigate and ameliorate the consequences of an attack and to assist the law enforcement community in gathering criminal evidence. Thus, we must build medical management capacities—including stockpiles of vaccines, antibiotics, and other supplies and systems for rapidly distributing these materials—and a system connecting the "front-end" awareness and assessment capacities to the "back-end" of the bioterrorism response system. Without robust capabilities for early detection and rapid assessment, the response to an act of bioterrorism may be ineffective or too late. As the recent anthrax incidents have shown, awareness and assessment capacities, particularly epidemiological and laboratory capacities, can be quickly overwhelmed. These capabilities, which were critical in assessing the risk of anthrax exposure, were slow to complete an assessment of risk despite knowing that an attack had occurred. The nature of future bioterrorist attacks may not be as readily apparent as the anthrax mailings have been. More covert attacks would place additional strains on the public health system to detect the attack, diagnose the agent and illness, and determine the scope of exposure and future course of the illness.

Surveillance

Early detection will be critical to saving lives. The sooner a bioterrorist event is detected, the sooner an assessment of the event can be completed, and the sooner medical care can be administered to those exposed. In the case of contagious diseases such as smallpox or pneumonic plague, detecting an outbreak early is essential to containing the outbreak. People today are incredibly mobile, commuting in and out of urban centers on a daily basis and traveling all over the world regularly. Failure to detect an outbreak of a contagious disease early could result in its rapid spread.

A national surveillance system to provide an early warning of unusual outbreaks of disease, both natural and intentional, will be a critical component of our preparedness. This system will depend on an information infrastructure that includes electronic data networks connecting local public health departments and area health care providers and providing regular analyses of the data for the presence of unusual trends that could indicate a bioterrorist attack. Additional sources of data that could provide an early indication of a bioterrorist attack include spikes in flu-like symptoms, over-the-counter drug sales, or absenteeism. The crucial element will be a robust information infrastructure for collecting, analyzing, and sharing information from all of these sources.

Epidemiology

Epidemiologists play an important role in surveillance and detection. They routinely monitor disease trends and take appropriate measures to meet potential public health threats. Epidemiologists will also be critical in determining the scope of the exposure to a bioterrorist agent once it has been detected. Typically, they trace

the outbreak back to its source, determine who was in the exposed area at the time of release, and recommend medical management measures. Because of the labor-intensive nature of epidemiology, which depends largely on interviews and analyses of disease trends, state departments of health will have to hire and train staff to be aware of natural outbreaks of disease as well as the wide range of bioterrorist agents.

Laboratory Requirements

Public health laboratories also play a critical role in the detection and assessment of bioterrorist incidents. A spike in requests for culture analyses from physicians could indicate an unusual outbreak of disease. Once an attack has been detected, laboratories will be critical in identifying the biological agent released. During the anthrax mailings, laboratories were called upon to determine which people in the proximity of the contaminated mail had been exposed and to assist law enforcement in gathering forensic evidence for prosecuting the perpetrator(s). Upgrading laboratory capacity by expanding advanced diagnostic capabilities, increasing the range of bioterrorist agents that can be identified at state and local laboratories, and making diagnostic exams faster and more accurate will be critical to an effective preparedness system.

Information and Communication

The underpinning for all of the components of an integrated detection, assessment, and response system will be a robust information infrastructure. Surveillance, epidemiology, and laboratory capacities for meeting the bioterrorist challenge will all depend on a robust information infrastructure. Information technology could be used to exchange procedural guidelines prior to a bioterrorist event, provide a mechanism for compiling and analyzing data on disease trends from different sources, share information during an event and lessons learned after an event, and provide training for all constituencies. In addition, accurate and timely information will be the backbone of the decision making process in times of crisis and will provide credible and consistent information to the general public to reduce panic. Bolstering and integrating existing information infrastructures to respond to bioterrorism will require expanding our technological infrastructure, as well as improving human and social understanding of how the infrastructure can be most effective.

Building Response Capacities

Any response system must have built-in flexibility so it can respond appropriately to a large-scale or small-scale event. Flexibility will require effective awareness and assessment tools that provide information on the nature of the attack so the response can be tailored appropriately. Local and federal responses should be based on a tiered, scalable approach commensurate with the scale of the attack.

Conclusions

Building and sustaining the public health system of systems described here will require sustained investment in people, technology, and materials. Adequate numbers of trained public health and medical personnel will be necessary to monitor the nation's health on an ongoing basis, operate and maintain the network of public health laboratories, investigate and analyze unusual outbreaks of disease, and provide preventive and therapeutic medical care for natural and intentional outbreaks. Building this system will also require investments in several key technologies, including the technologies for an electronic information infrastructure that can link federal, state, and local public health departments, hospitals, clinics, physicians' offices, and other medical care providers into a national public health network. Other technologies will be necessary to increase the speed and throughput of public health laboratories. An effective system of systems will also require adequate stocks of antibiotics, vaccines, and medical supplies—at both the national and local levels—to ensure that adequate treatment is available.

Creating and sustaining investments in people, technology, and materials will require strong partnerships between federal, state, and local governments, each of which will provide key capabilities in the public health system of systems. The role of the federal government will be to provide funding to support local and state preparedness and to take the lead as system integrator. A strong partnership between the public and private sectors—especially private health care institutions like hospitals and private-practice physicians—will also be important. The private sector should play a role, although the private sector cannot be expected to assist in planning for the mass distribution of medications or to maintain surge capacities for unlikely contingencies. That task will fall to state and local governments.

We need a system that will enable us to mobilize all of our health care resources rapidly wherever they are needed.

Cybercare: A System for Confronting Bioterrorism

Joseph M. Rosen; C. Everett Koop; Eliot B. Grigg

Joseph M. Rosen

C. Everett Koop

Eliot B. Grigg

Everything is not okay. On September 11, the realm of possibility suddenly expanded to include the unthinkable, and we were reminded that there are people who are willing and able to inflict massive civilian casualties in the United States. Moral repugnance is no longer a sufficient deterrent. September 11 also demonstrated that we cannot rely on prevention. We must be prepared to respond to a whole host of catastrophic contingencies.

The anthrax scare shortly thereafter introduced us to the threat of deadly biological agents. We were lucky this time, but 12 nations are known to possess, or are suspected of possessing, offensive biochemical weapons. The characteristics that make biological devices unwieldy as weapons of war—such as silence, incubation time, and uncontrollability—make them effective options for bioterror. Biological agents differ from their chemical and nuclear counterparts in a number of important ways: (1) they are easy to conceal; (2) if they are contagious, infected people can spread the disease; (3) the first responders exposed are likely to be health professionals rather than the traditional emergency personnel; (4) the longer an epidemic goes unrecognized and

Joseph M. Rosen is an associate professor of plastic and reconstructive surgery and an adjunct professor of radiology, Dartmouth Hitchcock Medical Center. C. Everett Koop is senior scholar and Elizabeth DeCamp McInerny Professor of Surgery at the C. Everett Koop Institute, Dartmouth College. Eliot B. Grigg is a teaching intern in the Thayer School of Engineering and research assistant, Institute for Security Technology Studies, Dartmouth College.

undiagnosed, the more difficult it is to control its effects. A well executed dispersal of an infectious pathogen would have devastating effects, and the psychological fallout and panic would be even worse.

As long as we value our personal freedoms, intelligence and law enforcement will never be perfect. In any case, although preventive measures are necessary, they can never be sufficient—no one can anticipate every contingency. In addition, because the intelligence community operates covertly, it can do little to allay popular fears or restrain panic. To meet this threat, we need a new strategy that brings together our command, communication, and control technologies. We must be able to mobilize all of our health care resources rapidly wherever the threat appears, even if it appears in many places simultaneously. During a crisis, there is no time to invent a response. We must be prepared, and right now we are not.

Threats

Six biological agents are most suitable for "weaponization": plague, tularemia, botulinum (toxin), the hemorrhagic fevers, anthrax, and smallpox. Three of the six, plague, the hemorrhagic fevers, and smallpox, can be transmitted from person to person. We will briefly discuss two of them—anthrax and smallpox—as examples.

Anthrax is caused by a bacterium, *Bacillus anthracis*. Infection can be manifested in three different forms: inhalational, cutaneous, and gastrointestinal anthrax. The mortality rate of occupationally acquired cases of anthrax in the United States is 89 percent. A 1993 report by the U.S. Congressional Office of Technology Assessment estimated that between 130,000 and 3 million deaths could follow the aerosolized release of 100 kg of anthrax spores upwind of the Washington, D.C., area—lethality matching or exceeding that of a hydrogen bomb (OTA, 1999). The military has a vaccine for anthrax, but current supplies are limited, production capacity is modest, and sufficient quantities of vaccine cannot be made available for civilian use for several years. Depending on the strain, anthrax usually responds to ciprofloxacin, doxycycline, or penicillin. However, anthrax exposed to less than lethal levels of any of these antibiotics is capable of developing resistance.

Smallpox, a disease caused by the variola major virus, was declared eradicated from the world as a naturally occurring disease in 1997. Routine vaccinations were discontinued in the United States in 1972 and in the rest of the world by 1979. Thus the vast majority of people everywhere have either never been vaccinated against the disease or have only partial immunity from vaccinations that were administered decades ago. Historically, the fatality rate from outbreaks of smallpox has been about 30 percent, but it is higher among the unvaccinated. Smallpox vaccine has been out of production for 30 years, and the government is not sure how far its reserve of 15 million doses can be diluted. There is no proven, effective, specific treatment for smallpox.

As long as we value our personal freedoms, intelligence and law enforcement will never be perfect.

Current Level of Preparedness

In testimony before the Senate Appropriations Subcommittee on Labor, Health and Human Services, and Education and Related Agencies, Tommy G. Thompson, Secretary of the U.S. Department of Health and Human Services, described our preparedness for a biological attack:

> *Let me characterize our status this way: we are prepared to respond … [September 11] is the first time our emergency response system had been tested at this extreme level, and it responded without a hitch . . . We were prepared to move rapidly to contain and treat any problematic disease . . . Our response encouraged me. It should encourage this committee and the Congress. And it should encourage the American public that we do have the ability to respond.*

However, Thompson also noted, "Granted, we did not find any signs of bioterrorism."

The first sizeable simulation of a national response to a biological attack took place in May 2000. The exercise, named TOPOFF because it involved top officials from all levels of government, involved a simulated, covert dispersal of an aerosol of plague at the Denver Performing Arts Center that was discovered three days later when plague was first diagnosed among a wave of flu-like cases

that cropped up in the Denver health care system.

On Day 1, a diagnosis of plague was confirmed by a state laboratory and the Centers for Disease Control (CDC). By Day 2 there was a state-wide shortage of ventilators and antibiotics. A federal "push pack" with antibiotics and other medical supplies arrived later that day, but transporting them from the Denver airport proved to be problematic. On Day 3 the state borders of Colorado were closed, but the question of feeding the four million inhabitants had not been thoroughly addressed. By the end of that day, overwhelmed by the influx of patients, medical care in Denver was beginning to shut down. On Day 4 there were an estimated 3,700 cases of plague and 950 deaths. At that point, the simulation was terminated. According to Thomas V. Inglesby, M.D., senior fellow at the Johns Hopkins Center for Civilian Biodefense Studies, "There were ominous signs at the end of the exercise. Disease had already spread to other states and countries. Competition between cities for the national pharmaceutical stockpile had already broken out. It had all the characteristics of an epidemic out of control."

We have been lucky so far, but luck cannot be the foundation for a public health policy.

The next major simulation, in June 2001, called Dark Winter, involved a simulated outbreak of smallpox in Oklahoma City. During the 13 days of the exercise, the disease spread to 25 states and 15 other countries. According to the ANSER Institute for Homeland Security, the lessons learned from this exercise were: (1) an attack on the United States with biological weapons could threaten vital national security interests; (2) current organizational structures and capabilities are not well suited for managing a biowarfare attack; (3) there is no surge capability in the U.S. health care and public health systems, the pharmaceutical industry, or the vaccine manufacturing industry; (4) dealing with the media will be a major, immediate challenge for all levels of government; (5) containing the spread of disease will present significant ethical, political, cultural, operational, and legal challenges (ANSER, 2001).

Both simulations were based on the assumption that current stores of antibiotics and vaccines would be effective against the biological agent. However, a group of researchers in Australia recently demonstrated that this assumption may no longer be valid. In an attempt to produce a contraceptive vaccine for mice using the mousepox virus, scientists discovered that "virus-encoded IL-4 not only suppresses primary antiviral cell-mediated immune response but also can inhibit the expression of immune memory responses" (Jackson et al., 2001). In other words, the trial substance not only made the disease more virulent by suppressing the immune system, but also rendered the vaccine ineffective.

The results of these and other experiments are widely available because, unlike the work of nuclear physicists or cryptographers working on national security, the work of biologists is not regulated. As more and more bioengineered bugs are created and tested, information about the science (e.g., genomic data) and equipment (e.g., DNA sequencers and synthesizers) used to create such organisms is becoming increasingly accessible. Considering the malign uses of data generated in legitimate projects, health care and defense experts are raising questions about this easy accessibility. Before we begin to regulate access to data, however, someone must determine which data are potentially dangerous (Aldous, 2001).

In short, we are not prepared to respond to a biological attack. We have been lucky so far, but luck cannot be the foundation for a public health or national security policy. We must seriously rethink the way we approach the whole notion of responding to a biological attack.

The Response

Four major challenges were revealed in the TOPOFF and Dark Winter exercises: (1) inefficient decision making (officials participated in conference calls with 50 to 100 people, which was highly inefficient and led to significant delays in action); (2) lack of coordination of emergency management (the absence of predetermined guidelines led to chaotic attempts at interagency communication); (3) lack of priorities and logistics for allocating resources (problems were encountered in accepting and distributing federal resources at the local level); and (4) security (especially at health care facilities, for enforcing a quarantine).

In a real emergency officials will need real-time

information tools that enable them to collect information and analyze it rapidly. The primary elements of an effective response to a biological attack must include: (1) detection/diagnosis; (2) quarantine/security; (3) resource mobilization/allocation; (4) panic management/media relations; and (5) command and control.

Cybercare

Cybercare, a new concept that takes advantage of the best new technologies, would be able to address all of these elements from the systems level to the specifics. The U.S. Department of Justice tasked the Institute for Security Technology Studies (ISTS) at Dartmouth College to make recommendations for planning a response to bioterrorism as part of its grant to study emerging terrorist threats. In January 2001, ISTS organized a conference that generated recommendations to strengthen and supplement public health infrastructure and formulate a national response plan to a terrorist attack. The plan would integrate a number of emerging technologies that collectively became known as "cybercare" (Rosen and Lucey, 2001).

Cybercare involves telemedicine, telesurgery (Madhani, 1997), telementoring, and distance learning systems. It also includes virtual reality simulators, augmented reality (Blackwell et al., 1998), datafusion, computer patient records, clinical information systems, and software intelligent agents. Cybercare can be thought of as cyberspace plus health care, a way of creating an entirely new environment for health care at a distance.

Detection/Diagnosis. There are two basic ways of detecting a biological attack. The first is to analyze epidemiological data; the second is to analyze biological samples in the field. The first was tested at President George W. Bush's inauguration in January 2001. A Defense Advanced Research Projects Agency (DARPA)-developed software program, known as ENCOMPASS (the enhanced consequence management planning and support system) was used to track the health conditions of all individuals who were treated at area military treatment facilities, Veterans Affairs medical clinics, civilian hospitals, and first aid stations between January 10 and February 4 in Washington, D.C., and surrounding counties. Participating health care personnel filled out brief forms when seeing patients to note whether they showed any of seven specific symptoms or complaints that might be indicative of outbreaks of illnesses, such as those caused by biological warfare agents. ENCOMPASS created a database of patient health records and matched spikes in certain clinical symptoms with specific geographic areas. At the inauguration, it detected a seasonal "outbreak" of the flu (Pueschel, 2001).

Cybercare can be thought of as cyberspace plus health care.

Laboratories around the country are trying to develop a portable detector that can diagnose field samples. The Lincoln Laboratory at the Massachusetts Institute of Technology (MIT) is developing a microchip combined with mouse B cells to detect individual pathogens (Pescovitz, 2000). Efforts are under way to increase the speed, sensitivity, and cost-effectiveness of such a detector. Other laboratories are also experimenting with innovative detection/diagnosis devices.

At the 2002 Winter Olympics in Salt Lake City, a combined approach called RAPID will be used. The system, which was developed by the U.S. Air Force in conjunction with Idaho Technologies, is a web-based surveillance system that analyzes patient records and uses 50-pound, backpack-sized portable laboratories to analyze field samples using polymerase chain reaction technology (Ault, 2001). Someday, large databases managed by intelligent software agents may be used to predict attacks before they happen (Graham-Rowe, 2001).

Quarantine/Security. In the event of a sizeable bioattack, some form of quarantine will be necessary. The major obstacle to imposing a quarantine is political, but even if it can be imposed, it will be difficult to enforce. Robots could be used for surveillance and, possibly, for enforcement (although we have a long way to go culturally for this to happen). Once a quarantine has been imposed, cybercare will be the most effective way of bringing in and managing outside resources as will be discussed in the next section.

Resource Mobilization/Allocation. In June 2001 another conference was held by ISTS on logistics and interagency communication in response to a hypothetical bioterror attack in Hanover, New Hampshire. As Figure 1 shows, resource mobilization was the primary

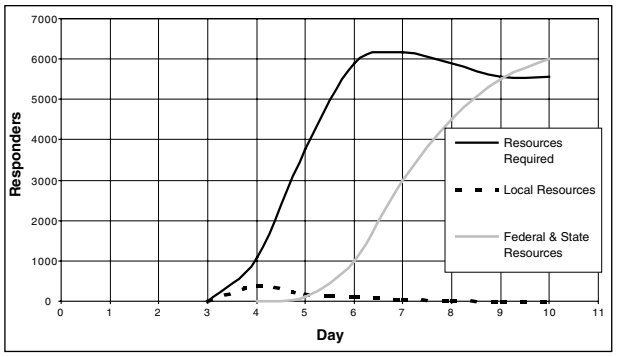

FIGURE 1 Assessing the bioterrorist threat.

challenge. The black line represents the estimated requirement for personnel in response to a biological incident involving 5,000 casualties infected with tularemia. Although available local resources (dashed line) would respond quickly, they would fall far short of the need, and they would rapidly become less effective from burnout. State and federal resources (gray line) would begin to reach the scene one to two days later. A severe shortage of resources during days five through eight would essentially preclude an effective response and would result in misery and chaos. The late-arriving state and federal personnel could deal with the horrendous aftermath but would not be involved in the direct response. The aftermath might be comparable to the result of an instantaneous nuclear explosion, and the mounting chaos would unfold before the eyes of the world on CNN for four or more days. Thus, overcoming the shortfall in resources in days five through eight would be critical to responding effectively to a biological incident. Keep in mind that tularemia is not even a contagious agent (Rosen et al., 2001).

The cybercare system would work on a one-to-one level, bringing together local providers in the affected areas and distant experts. At the same time, it would work on the highest level, enabling emergency workers to gain control over a large-scale disaster as quickly as possible (Figures 2 and 3). The system would provide real-time simulators for determining, on the run, the best options for deploying available resources. As the TOPOFF exercise showed, it can be much easier to get resources to an area in need (e.g., from Washington, D.C., to the Denver Airport) than to distribute the resources effectively.

In the event of a smallpox attack, remote monitoring will be important. To minimize the spread of infection, patients should be isolated in their homes or other non-hospital facilities whenever possible. Considering that doctors can only offer palliative care and support therapy, patients could reasonably remain at home. Ideally, remote monitoring could be done by robots, which could bridge the virtual and physical worlds.

A robot manipulated remotely could also distribute vaccines or gas masks. A company in Massachusetts, iRobot, has developed robots that can be controlled over the Internet and outfitted with cameras, as well as an array of sensors. One model, the Cobalt 2, could revolutionize videoconferencing by adding the controllable, physical presence of a robot. Telepresence, as it is called, enables a remote user to interact with and manipulate a distant environment as though he were physically present (Lanier, 2001).

FIGURE 2 Cybercare system illustrating multiple clinics providing care remotely.

Robots are already being tried in search-and-rescue operations. Immediately after September 11, 18 experimental robots were brought to New York from the University of South Florida to be used at the World Trade Center. Although they did not locate any survivors, the

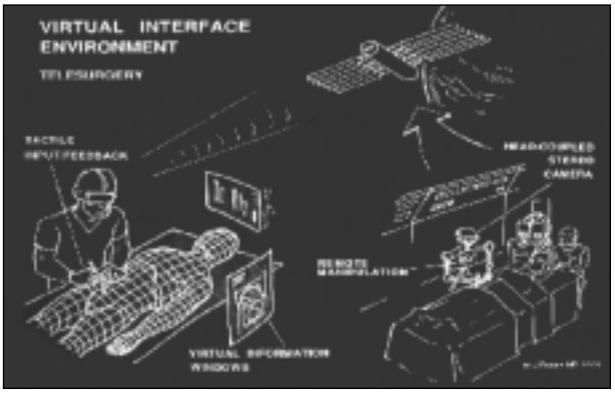

FIGURE 3 Telesurgery via satellite using haptics and robotics.

robots were small enough and durable enough to go places humans and dogs could not go. The robots were armed with a variety of sensors for locating survivors (e.g., heat sensors). In addition, the robots were expendable (Trivendi, 2001).

In a biological crisis, whatever actions can be performed remotely should be for several reasons. First, a remotely operated performer can move resources rapidly because it moves through virtual rather than physical space. Second, the operator can simultaneously call upon a large pool of resources regardless of time or place. Finally, the human operator avoids the risk of exposure to the hot zone. As artificial intelligence and other technologies improve, robots will become increasingly capable and autonomous.

Panic Management/Media Relations. This is the only element of the response to a biological attack that would be largely outside the realm of cybercare. However, to prevent panic outside of the hot zone, the public must be told what steps are being taken and assured that the situation is (or soon will be) under control. This can be done with effective information gathering and dissemination. To prevent panic within the hot zone, remotely operated robots could perform crucial tasks and minimize rescuer exposure.

Command and Control. This is the most important and complex element of the cybercare system. Indeed, it is the brains of the whole operation. Cybercare is a matrix that combines a number of different technologies in a telecommunications space. Ideally, a seamless connection would be maintained between information technologies connected to the physical world through robotics and information technologies connected to the virtual world. In a cybercare system, these two worlds would be different ways of expressing information technologies, either locally or at a distance.

In the cybercare model, sensors would gather information from many sources, including robots, software agents, human agents, medical records, epidemiological data, and resource data to name a few. The information would be conveyed in many forms: voice, data, video, or a combination of the three. The network ferrying the data must be flexible, redundant, expandable, largely wireless, and allow for high bandwidth; the massive amount of incoming data must be processed continually. To avoid information overload, the data would be filtered by intelligent software as well as faster-than-real-time simulations that could predict the outcomes of certain actions. Manipulating the mass of data will also require a new interface—a three-dimensional virtual space, such as a datacube, perhaps (Figure 4). This same interface would enable the remote manipulation of the hot zone. Over time, some parts of the cybercare system, such as robots and intelligent software, would become increasingly autonomous.

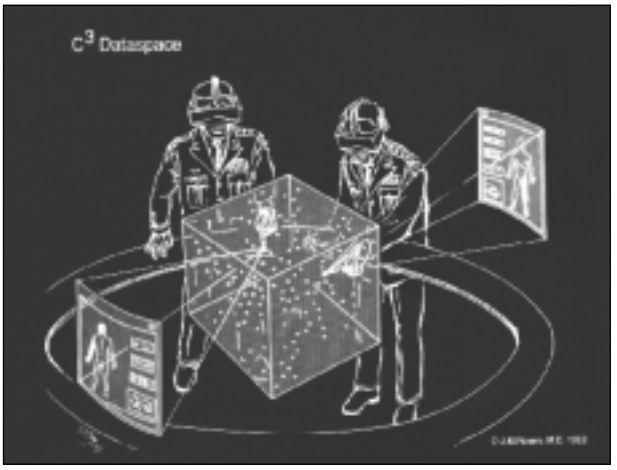

FIGURE 4 Command and control with a virtual datacube.

Command and control would coordinate the activities of competing federal, state, and local agencies, in addition to facilitating individual doctor-to-patient remote interactions. Therefore, like the rest of the cybercare system, command and control would be somewhat decentralized. The cybercare system would not dictate specific connections; rather, it would facilitate intracontinental connections. By condensing time and space, it would make possible a faster, broader, more coordinated, and ultimately more effective response to an attack.

The Future

Most of the technologies described so far are either available today or will be in a few years. As the system evolves, virtual reality will become the preferred mode of interaction and will be more closely coupled with physical reality to create a hybrid, augmented reality. When telepresence is replaced by teleimmersion, a user will have difficulty distinguishing between the local and remote environments. The ultimate goal is not to remove humans from the loop but to enable humans to use their time and abilities efficiently and to protect them from harm. Robots will become more integrated into normal society. They might, for example, be hung on walls, much like fire extinguishers, and, in an emergency, deploy automatically and act completely

autonomously. Whole cities might someday be covered in millions of sensors the size of dust particles. Eventually nanotechnology will change the rules once again.

Conclusion

We don't mean to minimize the institutional barriers that will have to be overcome for cybercare to become a reality. As Secretary Thompson said after September 11, public health is a "national security issue." The decentralization of health care delivery will be good for national security and, ultimately, in the interest of the U.S. government. At a similar time in history, Winston Churchill, deeply troubled by England's lack of preparation for World War II, said, "The responsibility of ministers for the public safety is absolute and requires no mandate. It is in fact the prime object for which governments come into existence."

A terrorist attack designed to cause catastrophic levels of casualties by spreading a contagious disease or chemical or radiation illness across America must be met with a health care system prepared to respond to worst-case scenarios and provide the surge capacity we will need in hours, not days. A cybercare system would protect the health of Americans, protect our economy, and, ultimately, protect our way of life. The creation of this new system will require a large-scale project that will certainly be expensive—but not as expensive as doing nothing. In addition, initial costs might be made up for in future savings. A cybercare system would take advantage of our strengths and could be developed rapidly if we start now.

In the interim, the infrastructure and technologies developed for a cybercare system would greatly improve the delivery of everyday health care. Reaching a remote, dangerous site is not very different from reaching a remote, rural site, and the technologies for a cybercare system would greatly increase access to health care. Whether it is designed to respond to a nuclear, chemical, or biological attack, a natural disaster, or simply to minimize travel costs and increase routine access to care, cybercare will be our future health care.

References

ANSER. 2001. Dark Winter: Summary. Available online at: <*http://www.homelandsecurity.org/darkwinter/index.cfm*>.

Aldhous, P. 2001. Biologists urged to address risk of data aiding bioweapon design. Nature 414: 237–238. Also available online at: <*http://www.nature.com/cgitaf/DynaPage.taf?file=/nature/journal/v414/n6861/full/414237a0_fs.html&content_filetype=pdf*>.

Ault, A. 2001. Olympics Rapid Response System. Wired 9(11): 4. Also available online at: <*http://www.wired.com/wired/archive/9.11/mustread.html?pg=4*>.

Blackwell, M., F. Morgan, and A.M. DiGioia III. 1998. Augmented reality and its future in orthopaedics. Clinical Orthopaedics and Related Research 354: 111–122.

Graham-Rowe, D. 2001. Intelligence analysis software could predict attacks. Available online at: <*http://www.newscientist.com/hottopics/bioterrorism/bioterrorism.jsp?id=ns99991368*>.

Jackson, R.J., A.J. Ramsay, C.D. Christensen, S. Beaton, D.F. Hall, and I.A. Ramshaw. 2001. Expression of mouse interleukin-4 by a recombinant ectromelia virus suppresses cytolytic lymphocyte responses and overcomes genetic resistance to mousepox. Journal of Virology 75: 1205–1210. Also available online at: <*http://www.micab.umn.edu/program/pdfs/jackson.pdf*>.

Lanier, J. 2001. Virtually there. Scientific American 284(4): 66–75. Also available online at: <*http://www.sciam.com/2001/0401issue/0401lanier.html*>.

Madhani, A. 1997. Design of Teleoperated Surgical Instruments for Minimally Invasive Surgery. Doctoral thesis, Massachusetts Institute of Technology.

OTA (Office of Technology Assessment). 1999. Proliferation of Weapons of Mass Destruction: Assessing the Risk. OTA-ISC-559. Washington, D.C.: U.S. Government Printing Office. Also available online at: <*http://www.wws.princeton.edu/cgi-bin/byteserv.prl/~ota/disk1/1993/9341/9341.PDF*>.

Pescovitz, D. 2000. Bioagent chip: a sensor to detect a biological warfare attack in seconds. Scientific American 282(3): 35. Also available online at: <*http://www.sciam.com/2000/0300issue/0300techbus4.html*>.

Pueschel, M. 2001. DARPA System Tracked Inauguration for Attack. Available online at: <*http://www.usmedicine.com/srticle.cfm?articleID=172&issueID=25*>.

Rosen, J., and C. Lucey, eds. 2001. Emerging Technologies: Recommendations for Counter-Terrorism. Hanover, N.H.: Institute for Security Technology Studies, Dartmouth College. Also available online at: <*http://thayer.dartmouth.edu/~engg005/MedDisaster/*>.

Rosen, J., R. Gougelet, M. Mughal, and R. Hutchinson. 2001. Conference Report of the Medical Disaster Conference, June 13–15, 2001. Hanover, N.H.: Dartmouth College. Also available online at: <*http://thayer.dartmouth.edu/~engg005/MedDisaster/*>.

Trivendi, B.P. 2001. Search-and-rescue robots tested at New York disaster site. Available online at: <*http://news.nationalgeographic.com/news/2001/09/0914_TVdisasterrobot.html*>.

Ensuring our cybersecurity will require long-term, innovative basic research.

Cybersecurity

Wm. A. Wulf and
Anita K. Jones

Wm. A. Wulf

Anita K. Jones

Although the nation is at great risk from cyberterrorism, we have virtually no research base on which to build truly secure systems. Moreover, only a tiny cadre of researchers are thinking deeply about long-term solutions to this problem. If the problem were merely a matter of implementing techniques that are known to be adequate, this might not be a serious issue. But the truth is that we do not know how to build secure computer systems. The only model widely used for cybersecurity is the "perimeter defense" model—which is demonstrably fragile. In fact, for deep theoretical reasons, it is impossible to guarantee that a perimeter-defense system will ever work! To be sure, many immediate problems of cybersecurity can be handled by implementing or enforcing known "best practices"—such as patching software each time a new attack is successful. But solving the fundamental problem will require long-term, innovative basic research.

No one knows how vulnerable we really are because the most costly attacks have not been made public. But we are probably a lot more vulnerable than we'd like to be, and maybe more vulnerable than we can survive! Financial cybersystems have been attacked but have not disclosed damage and losses in order to preserve an image of their integrity. Military systems have also been

Wm. A. Wulf is president of the National Academy of Engineering. Anita K. Jones is a member of the NAE and the Lawrence R. Quarles Professor of Engineering and Applied Science at the University of Virginia.

attacked, but the most serious attacks have not been disclosed. (It has been reported, however, that more than 60 percent of military computers have been compromised [GAO, 2001].) We know that national defense computers and networks use the same software and hardware as the general public—and thus are subject to the same kinds of attacks. In addition, they are a juicy target for sophisticated, state-sponsored intruders who want to determine our military preparedness.

To exacerbate things, our legal system prevents the exchange of information about attacks, thus preventing one organization from learning from the experiences of others. In anticipation of Y2K problems, Congress passed special legislation enabling corporations to exchange information (and limit liability). But no such legislation has been passed to permit the exchange of cybersecurity information. Other laws—laws to protect civil liberties, for example—prohibit the exchange of information among some government agencies. Although this is an admirable goal, it does make cybersecurity more difficult.

The bottom line is that no one knows exactly how vulnerable we are! We can get an idea of the magnitude of the problem, however, from public information. The 1997 Presidential Commission on Critical Infrastructure Protection focused on cybersecurity, although the commission's charter included power, water, communications, financial, and other infrastructures. In its report, the commission found that "all our infrastructures [are] increasingly dependent on information and communications systems …. [that] dependence is the source of rising vulnerabilities, and therefore, it is where we concentrated our efforts" (Presidential Commission on Critical Infrastructure Protection, 1997). In other words, all forms of infrastructure are so vulnerable that the commission decided to all but ignore other vulnerabilities. Information technology has become crucial to every aspect of modern life, and a serious attack could cripple any system, including systems used for an emergency military deployment, health care delivery, and the generation of electrical power.

National defense computers are a juicy target for sophisticated state-sponsored intruders.

The worst-case scenarios are chilling. Consider a really sophisticated attack on our financial systems. We're not talking about a simple virus, or even the theft of funds; we're talking about the incapacitation or destruction of parts of an infrastructure on which all commerce depends. Just imagine a month, a week, or even a day in which no checks are cashed or salaries deposited, no stocks are traded, no credit card purchases are honored or loans processed—in short, a day on which all commerce comes to a halt.

But the bottom line is that we don't know. Publicly reported attacks have been relatively unsophisticated and, although annoying, have not had dire consequences. The unreported attacks have been more serious, but the details have not been made known to the public—or, in some cases, even to the responsible public officials. Potential attack scenarios are even worse—but the probability that they will happen is simply not known.

Our critical systems have many vulnerabilities, ranging from errors in software to trusted, but disgruntled, employees to low-bid software developers outside the United States. But the problem goes much deeper. In many cases, attackers have found clever ways to combine two or more features of a system in ways the designers had not foreseen. In these cases, undesirable behavior results from correctly implemented software. In addition, software vendors have found that the public is not willing to pay for security. Buyers do not choose more secure products over less secure ones, especially if they must pay a premium for them, so venders have not invested in security. But the overriding, fundamental source of vulnerability is that we do not have a deep understanding of the problem or its solution; and little if any research is being done to develop that understanding.

How prepared are we to respond? There are different answers for the short term and the long term, and to some extent there are different answers for the military, the private sector, financial institutions, and other communities. Unfortunately, the only short-term solution is to keep putting our fingers in the dike—to patch holes in systems as we discover them. To be effective, this requires that every member of a vast army of system administrators and users be vigilant. Alas, the evidence shows that widespread vigilance is extraordinarily hard to achieve.

Equally unfortunate, the Internet is essentially a monoculture—almost all of the computers connected to it are IBM compatible. Because they use a single operating system and set of applications, a would-be attacker only has to find a vulnerability in any part of the system to attack the vast majority of computers connected to the network. That is why attacks all seem to spread so rapidly.

One of the principal findings of the Presidential Commission on Critical Infrastructure Protection was that research and development are not adequate to support infrastructure protection. For historical reasons, no single federal funding agency has assumed responsibility for supporting basic research in this area—not the Defense Advanced Research Projects Agency, not the National Science Foundation, not the U.S. Department of Energy, and not the National Security Agency. As a result, only relatively small, sporadic research projects have been funded, and the underlying assumptions on cybersecurity that were established in the 1960s mainframe environment have not be questioned. When funds are scarce, researchers become very conservative, and bold challenges to the conventional wisdom are not likely to pass peer review. As a result, incrementalism has become the norm. Thus, no long-term cybersecurity solution has been developed, or even thoroughly investigated.

Four critical needs must be met to improve cybersecurity:

- the need for a new model to replace the perimeter defense model
- the need for a new definition of cybersecurity
- the need for an active defense
- the need for coordinated activities by cybercommunities, legal system, and regulatory systems

A New Model

Most research on cybersecurity has been based on the assumption that the "thing" we need to protect is "inside" the system. Therefore, we have developed "firewalls" and other mechanisms to keep "outside" attackers from penetrating our defenses and gaining access to the thing and taking control of the system. This perimeter defense model of computer security—sometimes called the Maginot Line model—has been used since the first mainframe operating systems were built in the 1960s. Unfortunately, it is dangerously, even fatally, flawed.

First, like the Maginot Line, it is fragile. In WWII, France fell in 35 days because of its reliance on this model. No matter how formidable the defenses, an attacker can make an end run around them, and once inside, can compromise the entire system. Second, the model fails to recognize that many security flaws are "designed in." In other words, a system may fail by performing exactly as specified. In 1993, the Naval Research Laboratory did an analysis of some 50 security flaws and found that nearly half of them (22) were designed into the requirements or specifications for correct system behavior! Third, a perimeter defense cannot protect against attacks from inside. If all of our defenses are directed outward, we remain vulnerable to the legitimate insider. Fourth, major damage can be done without "penetrating" the system. This was demonstrated by the distributed denial-of-service attacks on Yahoo and other Internet sites two years ago. Simply by flooding the system with false requests for service, it was rendered incapable of responding to legitimate requests. We can be grateful that so far denial-of-service attacks have been directed against Internet sites and not against 911 services in a major city! Fifth, the Maginot Line model has never worked! Every system designed with a Maginot Line-type notion of security has been compromised—including the systems the authors built in the 1970s. After 40 years of trying to develop a foolproof system, it's time we realized that we are not likely to succeed. Finally, the perimeter defense cannot work for deep theoretical reasons. Unfortunately, we don't have enough space here to explain. Suffice it to say that replacing the perimeter defense model of computer security is long overdue!

The perimeter defense model is dangerously, even fatally, flawed.

Redefinition of Cybersecurity

The second critical need for cybersecurity is to redefine "security." The military definition of security emphasizes controlling access to sensitive information. This is the basis of the compartmentalized, layered

(confidential, secret, top secret) classification of information. A somewhat broader definition of security used in the computing research community includes two other notions: "integrity" and "denial of service." Integrity implies that an attacker cannot modify information in the system. In some cases, medical records for instance, integrity is much more important than secrecy. We may not like it if other people see our medical records, but we may die if someone alters our allergy profile. Denial of service means that the attacker does not access or modify information but denies users a service provided by it. This relatively unsophisticated form of attack can be used against phone systems (e.g., 911), financial systems, and, of course, Internet hosts. Because more than 90 percent of military communications are sent via the public telephone network, attackers might seriously disrupt a military activity, a deployment say, simply by tying up the phone lines at appropriate bases and logistics centers.

The line between sensitive and nonsensitive information is often blurred in cyberspace.

Practical definitions of security must be more sophisticated than the simple privacy, integrity, and denial of service formula, and they must be tailored for each kind of entity—systems for credit cards, medical records, tanks, flight plans, student examinations, and so forth. The notion of restricting access to a credit card to individuals with, say, secret clearance is nonsensical. Other factors, such as the timing, or at least the temporal order, of operations, correlative operations on related objects, and so on, are essential concepts for real-world security. (It used to be said that the best way to anticipate major U.S. military operations was to observe any increases in pizza deliveries to the Pentagon).

The military concept of sensitive but unclassified information has a counterpart in the cyberworld. Indeed, the line between sensitive and nonsensitive information is often blurred in cyberspace. In principle, one must consider how any piece of information might be combined with any other pieces of information to compromise our security. With the vast amount of information available on the Internet and the speed of modern computers, it has become all but impossible to anticipate how information will be combined or what inferences can be drawn from such combinations.

Different information sets stored in the same computer must be protected differently. The new model of cybersecurity should be appropriate to the context of the user applications for which that information is used. The simple model of a "penetration" attack does not reflect these realistic security concerns. Hence, analyzing the vulnerability of a system in terms of the perimeter defense model is unlikely to reveal its true vulnerabilities.

Active Defense

The third critical need for cybersecurity is for an active defense. Not all experts agree, but based on our experience over the past 30 years, we have concluded that a passive defense alone will not work. Effective cybersecurity must include some kind of active response—a threat or a cost higher than the attacker is willing to pay—to complement the passive defense.

Developing an active defense will be difficult because identifying the source of an attack is difficult. The practical and legal implications of active defenses have not been determined, and the opportunities for mistakes are legion. The international implications are especially troublesome. It is difficult, usually impossible, to pinpoint the physical location of an attacker. If it is in another country, a countermeasure by a U.S. government computer might even be considered an act of war. Resolving this and related issues will require a thoughtful approach and careful international diplomacy. We desperately need long-term basic scholarship in this area.

Coordinated Activities

Any plan of action must also involve a dialog on legal issues, the fourth critical need for cybersecurity. At least two kinds of issues should be addressed soon: (1) issues raised in cyberspace that do not have counterparts in the physical world; and (2) issues raised by place-based assumptions in current law. The first category includes everything from new forms of intellectual property (e.g., databases) to new forms of crime (e.g., spamming). Issues of particular interest to this discussion are rights and limitations on active countermeasures to intrusions—indeed, determining what constitutes an intrusion. Issues raised by place-based assumptions in current law include many basic questions. How does the

concept of jurisdiction apply in cyberspace? For tax purposes (e.g., sales taxes), where does a cyberspace transaction take place? Where do you draw the line between national security and law enforcement? How do you apply the concept of *posse comitatis*?

Not all of these issues are immediately and obviously related to cybersecurity. But cyberspace protection is a "wedge issue" that will force us to rethink some fundamental ideas about the role of government, the relationship between the public and private sectors, the balance between rights of privacy and public safety, and the definition of security.

The security of our information infrastructure and other critical infrastructures will be a systems problem, as well as a significant research challenge. We believe that a particular government agency must take on the mission of revitalizing research in cybersecurity with the following objectives:

- the development of wholly new methods of ensuring information system security
- the development of a larger research community in cybersecurity
- the education of computer system and computer science majors in cybersecurity at the undergraduate level, which would eventually improve the state of the practice in industry

Achieving these goals will require a guarantee of sustained support over a long period of time as an incentive to researchers to pursue projects in this area.

In the past few months, members of the House Science Committee have held hearings[1] on the state of research on cybersecurity and have introduced three acts that would provide initial funding for basic research through the National Science Foundation and the National Institute of Standards and Technology.[2] Although these initiatives are heartening, their full impact will not be felt for a decade or more. Historically, policy makers have not continued to support research with such long horizons. However, in the aftermath of September 11, we are hopeful that Congress is now ready to provide stable, long-term funding for this high-risk research.

References

GAO (General Accounting Office). 2001. Combating Terrorism: Actions Needed to Improve DOD Antiterrorism Program. Washington, D.C.: General Accounting Office.

Presidential Commission on Critical Infrastructure Protection. 1997. Critical Foundations: Protecting America's Infrastructures. Washington, D.C.: U.S. Government Printing Office.

[1] 1 For the text of written testimony by Wm. A. Wulf, see the NAE website <*www.nae.edu*> under "News & Events/National Academy of Engineering Counterterrorism Activities."

[2] H.R. 3316 Computer Security Enhancement and Research Act of 2001, H.R. 3394 Cyber Security Research and Development Act, and H.R. 3400 Networking and Information Technology Research Advancement Act.

NAE News and Notes

Class of 2002 Elected

In February the National Academy of Engineering (NAE) elected 74 members and 7 foreign associates. This brings the total U.S. membership to 1,857 active members and 250 members emeriti, and the number of foreign associates to 158. Election to the NAE is one of the highest professional distinctions that can be accorded an engineer. Academy membership honors those who have made "important contributions to engineering theory and practice" and those who have demonstrated "unusual accomplishment in the pioneering of new and developing fields of technology." A list of newly elected members and foreign associates follows, with their primary affiliations at the time of election and a brief statement of their principal engineering accomplishments.

New Members

Rakesh Agrawal, chief engineer, process synthesis, Air Products and Chemicals, Inc., Allentown, Pennsylvania, "for contributions to the development and worldwide implementation of high-efficiency and high-purity cryogenic and noncryogenic gas separation processes."

William F. Banholzer, vice president, global technology, GE Plastics, Pittsfield, Massachusetts, "for breakthroughs in stealth materials and contributions to the isotope effect in solid-state physics and for business leadership."

Frank S. Bates, professor and head, Department of Chemical Engineering and Materials Science, University of Minnesota, Minneapolis, "for important contributions on the phase behavior of polymer blends, particularly block copolymers."

James A. Brierley, chief microbiologist and chief research scientist, Newmont Mining Corporation, Englewood, Colorado, "for recognizing the potential of high-temperature biomining and for innovative industrial biomining practices."

C. Jeffrey Brinker, senior scientist, Inorganic Materials Chemistry Division, Sandia National Laboratories, Albuquerque, New Mexico, "for outstanding contributions to the science of sol-gel processing and the invention of porous materials with controlled structure."

Andrew Brown, Jr., director of engineering, Delphi Automotive Systems, Troy, Michigan, "for the effective planning and integration of large-scale, highly diverse research and engineering activities."

Joe C. Campbell, Cockrell Family Regents Chair in Engineering, University of Texas at Austin, "for contributions to the development of high-speed, low-noise avalanche photodiodes."

Michael J. Carey, technical director, FrameWork Development Division, BEA Systems, Inc., San Jose, California, "for contributions to the design, implementation, and evaluation of database systems."

Subrata K. Chakrabarti, president, Offshore Structure Analysis, Inc., Plainfield, Illinois, "for major contributions to the field of hydrodynamics and fluid structure interaction in the design of harbor, coastal, and offshore structures."

Morris Chang, chairman and chief executive officer, Taiwan Semiconductor Manufacturing Company, Taipei, "for contributions to the integrated circuit industry, the creation of the pure-foundry business model, and the enabling of the fabless semiconductor industry."

Douglas M. Chapin, president and director, MPR Associates, Inc., Alexandria, Virginia, "for improvements in reliability and the prevention and mitigation of core damage accidents in nuclear reactors worldwide."

Andrew R. Chraplyvy, director, lightwave systems research, Bell Laboratories, Lucent Technologies, Holmdel, New Jersey, "for contributions to the development of high-capacity optical fiber communication systems."

Joseph M. Colucci, president, Automotive Fuels Consulting, Inc., Clarkston, Michigan, "for leadership at the 'fuel/vehicle system' interface leading to improved automotive fuel and vehicle quality and reduced emissions."

Ross B. Corotis, chair, Department of Civil Engineering, University of Colorado, Boulder, "for the application of probabilistic modeling in design, new methods of reliability assessment and optimization of structures, and innovations in engineering education."

Henry Cox, chief scientist and senior vice president, ORINCON Corporation, Arlington, Virginia,

"for outstanding contributions to the performance of U.S. Navy sonars and the development of undersea acoustic superiority."

John H. Crawford, director of microprocessor architecture, Intel Corporation, Santa Clara, California, "for the architectural design of widely used microprocessors."

John C. Crittenden, Presidential Professor, Department of Civil and Environmental Engineering, Michigan Technological University, Houghton, "for the development of theory and the application of processes for removing toxic organic compounds from air and drinking water."

Edward L. Cussler, Institute of Technology Distinguished Professor of Chemical Engineering, University of Minnesota, Minneapolis, "for pioneering research on membrane transport in chemical and biochemical separation and for inspiring teaching."

Ruth A. David, president and chief executive officer, ANSER, Arlington, Virginia, "for pioneering the use of digital information technologies for testing, simulations, information processing, and telecommunications for high-capacity, high-reliability applications."

Robert E. Dickinson, professor, earth and atmospheric sciences, Georgia Institute of Technology, Atlanta, "for pioneering contributions to a wide range of topics in atmospheric dynamics and earth system modeling."

Bonnie J. Dunbar, assistant director for university research and affairs, NASA Johnson Space Center, Houston, Texas, "for personal leadership and significant contributions to the solution of engineering design problems in human space flight and to on-orbit operations."

Farouk El-Baz, professor and director, Center for Remote Sensing, Boston University, "for selecting the landing sites for the Apollo missions and for pioneering methods of discovering subsurface freshwater from space observations."

Robert E. Fontana, Jr., research staff member, IBM Almaden Research Center, San Jose, California, "for contributions to microfabrication techniques for the manufacture of thin-film storage devices."

Howard Frank, dean, College of Business and Management, University of Maryland, College Park, "for contributions to the design and analysis of computer communication networks."

Robert W. Galvin, chairman of the Executive Committee, Motorola, Inc., Schaumburg, Illinois, "for leadership in the commercialization of innovative electronics technologies and for advancing the principles of Total Quality Management."

Jacques S. Gansler, professor and Roger C. Lipitz Chair, Center for Public Policy and Private Enterprise, School of Public Affairs, University of Maryland, College Park, "for public and private leadership in the U.S. Department of Defense and major contributions in teaching missile guidance and control systems."

Fred W. Glover, professor of systems science, Leeds School of Business, University of Colorado, Boulder, "for contributions to optimization modeling, and algorithmic development, and for solving problems in distribution, planning, and design."

Thomas E. Graedel, professor of industrial ecology, Yale University, New Haven, Connecticut, "for outstanding contributions to the engineering theory and practice of industrial ecology, particularly for improved methods of life-cycle analysis."

William H. Hansmire, principal, Jacobs Associates, San Francisco, California, "for pioneering leadership in the integration of the design and construction of tunneling projects, including the first design-build demonstration project for the U.S. Department of Transportation."

Ronald K. Hanson, chair, Department of Mechanical Engineering, Stanford University, Stanford, California, "for the development and application of innovative laser diagnostics and sensors in the fields of combustion, chemical kinetics, and power conversion."

Alan J. Heeger, professor, Institute for Polymers and Organic Solids, University of California, Santa Barbara, "for cofounding the field of conducting polymers and for pioneering work in making these novel materials available for technological applications."

Martin E. Hellman, professor emeritus of electrical engineering, Stanford University, Stanford, California, "for contributions to the theory and practice of cryptography."

W.S. Winston Ho, professor, Department of Chemical and Materials Engineering, University of Kentucky, Lexington, "for the invention and commercialization of novel separation technologies and the development of new theoretical models for membrane separations."

Berthold K.P. Horn, professor, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, "for contributions to computer vision, including the recovery of three-dimensional geometry from image intensities."

Roland N. Horne, professor and

chair, Department of Petroleum Engineering, Stanford University, Stanford, California, "for innovations in the development of techniques for the testing and optimization of petroleum reservoirs."

Edward E. Horton, president, Deepwater Technologies, Houston, Texas, "for innovative contributions to the development of systems and structures for oil drilling and production in very deep water."

Evelyn L. Hu, professor, electrical and computer engineering, University of California, Santa Barbara, "for contributions to the processing of semiconductor structures and devices."

Klavs F. Jensen, Lammot duPont Professor of Chemical Engineering and professor of materials science and engineering, Massachusetts Institute of Technology, Cambridge, "for fundamental contributions to multiscale chemical reaction engineering with important applications to microelectronic materials processing and microreactor technology."

James T. Kajiya, assistant director of research, Microsoft Corporation, Redmond, Washington, "for contributions to formal and practical methods of computer image generation."

Adib K. Kanafani, Edward G. and John R. Cahill Professor of Civil Engineering and chairman, Department of Civil and Environmental Engineering, University of California, Berkeley, "for significant contributions to national and international air transportation, development of U.S. research on intelligent transportation, and the education of transportation professionals."

James C. Keck, Ford Professor of Engineering Emeritus and senior lecturer, Massachusetts Institute of Technology, Cambridge, "for developing innovative, widely used new concepts for modeling coupled chemical and physical phenomena in engine combustion and high-temperature flows."

Kenneth H. Keller, director, Center for Science, Technology, and Public Affairs, and professor of chemical engineering and materials science, University of Minnesota, Minneapolis, "for leadership in applying quantitative engineering analysis to vascular transport and artificial organ design and in public policy."

Chung K. (Ed) Law, Robert H. Goddard Professor, Department of Aerospace and Mechanical Engineering, Princeton University, Princeton, New Jersey, "for prolific and outstanding contributions to the understanding of the fundamentals of combustion processes and theory and their applications in propulsion systems."

David M. Lederman, president and chief executive officer, ABIOMED, Inc., Danvers, Massachusetts, "for designing, developing, and commercializing heart failure assist and heart replacement devices, and for leadership in engineering science education."

Mark J. Levin, chief executive officer, Millennium Pharmaceuticals, Inc., Cambridge, Massachusetts, "for contributions to animal cell bioprocess scale-up, and for entrepreneurial leadership in biotechnology, specifically genomics."

Bede Liu, professor, Department of Electrical Engineering, Princeton University, Princeton, New Jersey, "for contributions to the analysis and implementation of digital signal processing algorithms."

Alan G. MacDiarmid, Blanchard Professor of Chemistry, University of Pennsylvania, Philadelphia, "for the codiscovery and development of conductive polymers."

Bernard S. Meyerson, IBM fellow and vice president, IBM Thomas J. Watson Research Center, Yorktown Heights, New York, "for the development of low temperature epitaxy of SiGe for the fabrication of heterojunction, bipolar, integrated circuits for telecommunications."

A. Stephen Morse, professor of electrical engineering, Yale University, New Haven, Connecticut, "for contributions to geometric control theory, adaptive control, and the stability of hybrid systems."

Brij M. Moudgil, professor of materials science and engineering, and director, Engineering Research Center for Particle Science and Technology, University of Florida, Gainesville, "for advances in mineral processing through innovations in selective polymer and surfactant coatings and for professional leadership."

Gérard A. Mourou, A.D. Moore Distinguished University Professor of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, "for the introduction of the chirped pulse amplification technique enabling high-intensity lasers."

Cherry A. Murray, senior vice president, physical sciences research, Bell Laboratories, Lucent Technologies, Murray Hill, New Jersey, "for seminal work on order-disorder transitions in colloidal systems, and for leadership in bringing new concepts from research to production."

Thomas M. Murray, Montague-Betts Professor of Structural Steel Design, Virginia Polytechnic Institute and State University, Blacksburg, "for leadership in developing criteria for floor serviceability and major contributions to structural-steel design engineering practice."

Gordon C. Osbourn, senior

scientist and team leader, vision science, pattern recognition, and multisensor algorithms, Sandia National Laboratories, Albuquerque, New Mexico, "for originating the field of strained-layer superlattices and related structures, which has led to revolutionary advances in electronics and optoelectronics."

Christos H. Papadimitriou, chairman, Computer Science Division, Department of Electrical Engineering and Computer Science, University of California, Berkeley, "for contributions to complexity theory, database theory, and combinatorial optimization."

Neil E. Paton, chief technology advisor, Liquidmetal Technologies, Lake Forest, California, "for contributions to the development of advanced aluminum and high-temperature alloys for aerospace applications."

P. Hunter Peckham, professor of biomedical engineering, Case Western Reserve University, Cleveland, Ohio, "for developing implantable neuroprostheses to restore movement and independent function to paralyzed individuals."

Stephen M. Pollock, professor and past chair, Department of Industrial and Operations Engineering, University of Michigan, Ann Arbor, "for contributions to the education, science, and analysis of public and private sector operational systems."

Buddy D. Ratner, professor and director, Engineered Biomaterials Center, University of Washington, Seattle, "for contributions to the understanding of the surface interactions of biological molecules and cells with medical implants."

Arye Rosen, distinguished member, technical staff, Sarnoff Corporation, Princeton, New Jersey, "for contributions to microwave and laser technologies and the medical applications of these technologies."

Murray B. Sachs, Massey Professor and director, Whitaker Biomedical Engineering Institute, Johns Hopkins University, Baltimore, Maryland, "for contributions to the understanding of the neural encoding and signal processing of complex sounds and for leadership in bioengineering education."

Edmund O. Schweitzer III, president, Schweitzer Engineering Laboratories, Inc., Pullman, Washington, "for technical innovation in power system protection and technology transfer leading to the commercialization of products in the electric power industry."

William A. Sirignano, professor of mechanical and aerospace engineering, University of California, Irvine, "for contributions to the science and technology of spray combustion systems for propulsion."

Richard M. Stallman, president and founder, Free Software Foundation, Inc., Boston, Massachusetts, "for starting the GNU project, which produced influential, nonproprietary software tools, and for founding the free software movement."

Subra Suresh, professor and head, Department of Materials Science and Engineering, Massachusetts Institute of Technology, Cambridge, "for the development of mechanical behavior theory and experiment for advanced materials and applications and for demonstrating fruitful new avenues for structural study."

Rodney J. Tabaczynski, director, Powertrain and Vehicle Research, Ford Research Laboratory, Ford Motor Company, Dearborn, Michigan, "for major contributions to the understanding of processes in internal combustion engines resulting in improved performance and pollution control."

David W. Thompson, chairman of the board, president, and chief executive officer, Orbital Sciences Corporation, Dulles, Virginia, "for technical leadership in the conception and realization of small, flexible launch systems and spacecraft."

Moshe Y. Vardi, professor, Department of Computer Science, Rice University, Houston, Texas, "for contributions to the formal verification of hardware and software correctness."

Kenneth L. Walker, vice president, Specialty Fiber Devices Business Unit, and chief technical officer, Network Cable Systems, Lucent Technologies, Somerset, New Jersey, "for innovation and leadership in the fundamental understanding and process development for optical fibers and fiber devices."

Warren M. Washington, senior scientist and head, Climate Change Research Section, National Center for Atmospheric Research, Boulder, Colorado, "for pioneering the development of coupled climate models, their use on parallel supercomputing architectures, and their interpretation."

Elaine J. Weyuker, technology leader, AT&T Labs-Research, Florham Park, New Jersey, "for contributions to software testing, reliability, and measurement and for the development of mathematical foundations for software testing."

Donald C. Winter, president and chief executive officer, TRW Systems, Reston, Virginia, "for pioneering contributions to high-powered laser technology and defense applications."

M. Gordon Wolman, professor, Department of Geography and Environmental Engineering, Johns

Hopkins University, Baltimore, Maryland, "for outstanding contributions in fluvial processes, water resources management and policy, and environmental education."

Stephen Wozniak, Unuson Corporation, and cofounder, Apple Computer, Inc., Los Gatos, California, "for the invention and development of the first mass-produced personal computer."

Foreign Associates

Hiroyuki Abe, president, Tohoku University, Sendai, Japan, "for outstanding contributions in the extraction of geothermal energy and leadership in the development of nondestructive evaluation and electronic packaging techniques."

Brian D.O. Anderson, director of research, School of Information Sciences and Engineering, and professor of systems engineering, The Australian National University, Canberra, "for contributions to system and control theory and for international leadership in promoting engineering science and technology."

J. David Embury, professor, Department of Materials Engineering, McMaster University, Hamilton, Ontario, Canada, "for outstanding contributions to fundamental structure/mechanical-property relations of materials and their applications."

Vladimir E. Fortov, academician and vice president, Russian Academy of Sciences, Moscow, "for pioneering research of hot, dense matter under extreme conditions, and for reforming and energizing engineering in Russia's civilian sector."

Brian W. Kernighan, professor, Department of Computer Science, Princeton University, Princeton, New Jersey, "for contributions to software and to programming languages."

Maria-Regina Kula, professor and director, Institute of Enzyme Technology, Heinrich Heine University Düsseldorf, Jülich, Germany, "for contributions to the understanding and practice of enzyme-based chemical processes and protein separations."

Norbert Peters, professor, Center for Turbulence Research, Stanford University, Stanford, California, "for contributions to the field of combustion modeling of turbulent flames and the development of chemical kinetic mechanisms for hydrocarbon oxidation."

2003 Election Timetable

2002

February 20
Nomination packets available from the NAE Membership Office

April 12
DEADLINE for receipt of revised 2002 nominations and reference materials for candidates eligible for membership in 2003

May 10
DEADLINE for receipt of new nominations for membership in 2003

June 7
DEADLINE for receipt of reference forms for new nominations for membership in 2003

July 3
Member Comments packets mailed to all members

July 31
DEADLINE for receipt of Member Comments materials

October 5
Peer Committee meetings in Washington, D.C.

December 6–7
Committee on Membership meeting at the Beckman Center, Irvine, California

2003

January 3
Ballot book mailed to all active NAE members

January 30
DEADLINE for receipt of ballots

February 14
Class of 2003 election press release and 2004 election Quick Reference Guide mailed

NAE Thanks Donors

Sheila E. Widnall

The National Academy of Engineering has just ended the best fundraising year in its history. On our way to a 2001 goal of $18 million, the NAE received new gifts of more than $15.4 million from members, friends, and corporations on our way to a campaign goal of $65 million.

Since September 11, private philanthropy has become more important to us than ever. The NAE has drawn on unrestricted funds to convene a closed meeting of policy experts and to initiate programs in advance of specific government requests. We have also continued to work on other important projects, including new programs in engineering education, energy policy, public and media awareness, and health care delivery. None of these programs would be possible without the generous donations of 462 NAE members to the Annual Fund in 2001. (Contributors are listed on pages 52–56.) New gifts for NAE programs totaled $551,000. Our goal for 2002 is to increase that figure to at least $600,000, with 30 percent of NAE members participating.

The largest gift (and the largest gift in the National Academies campaign) in 2001 was a $10 million commitment by **Bernard Gordon** to create a national prize for innovation in engineering and technology education. Bernie's gift is a major component of our nascent program in engineering education. Because young, well trained engineers are essential to the continued technical and economic health and progress of our nation, the NAE has taken a particular interest in improving engineering education. In response to growing concerns about the steady decline in engineering enrollments, the NAE hopes to ensure the vitality and currency of the engineering education enterprise.

Private philanthropy is also allowing us to increase our program activities without adding large numbers of permanent staff. This year, **Thomas V. Jones** provided funds for a new fellowship in the NAE Program Office, allowing us to recruit an outstanding senior executive to lead one of our new initiatives. With Tom's gift, and an accumulation of other donations, endowment funds, and contract funds, we now have seven fellows and senior scholars. These experienced professionals are providing leadership in programs related to Department of Defense R&D, advances in nanotechnology, the role of ethics in engineering, new approaches to risk management, and counterterrorism.

Another program supported by contributions from NAE members is the Public Understanding of Engineering Program. Drawing on a grant from the Elizabeth and **Stephen D. Bechtel, Jr.**, Foundation, we hired our first media and public relations specialist, Randy Atkins. Randy is already making sure that the NAE is providing engineering expertise to the media to help shape the nation's response to terrorism. We are also grateful to **Ruben Mettler** for supporting our collaboration with the Foundation for American Communications (FACS), which conducted a valuable media-relations training session at this year's Annual Meeting. Earlier this month, FACS and the NAE cosponsored a one-day conference for managing editors of newspapers, radio, and television stations throughout the eastern United States.

In the next six months, every NAE member will be asked as part of the National Academies campaign to consider making a multiyear pledge to the NAE. I encourage you to begin thinking now about the potential impact your gift could have on the NAE and the national engineering enterprise. I hope you will join me and many other NAE members in becoming part of the Academy's Golden Bridge Society, which recognizes members who contribute $20,000 or more.

Wm. A. Wulf, the NAE Council, and I do not make these requests lightly. To increase the NAE's impact and visibility, we must have funds to support self-initiated program activities, and we must create an endowment to support future activities. We thank you for your contributions in 2001 and look forward to your continuing support in 2002.

Sheila E. Widnall, NAE Vice President
Institute Professor
Massachusetts Institute of Technology

National Academy of Engineering

2001 Private Contributions

Because of the disruption in mail service in Washington, D.C., the NAE is still receiving gifts with October, November, and December 2001 postmarks. If you mailed a gift and have not been included on this list, please contact the Development Office at 202-334-2431 or giving@nationalacademies.org. A final version of this list will be available later in 2002.

Golden Bridge Society

The Golden Bridge Society recognizes the generosity of current members who have made cumulative contributions of $20,000 or more, as well as planned gifts of any size made prior to January 2002. This list is organized by gift level.

$1,000,000 or more

Section 1

Norman R. Augustine

Section 3

Arnold O. Beckman
Ralph Landau

Section 4

Stephen D. Bechtel, Jr.

Section 7

Bernard M. Gordon
William R. Hewlett*
Gordon E. Moore

Section 8

Jordan J. Baruch

$100,000 to $999,999

Section 1

William F. Ballhaus, Sr.
Thomas V. Jones
Ruben F. Mettler
Robert H. Wertheim

Section 2

Alejandro Zaffaroni

Section 3

William L. Friend

Section 5

John A. Armstrong
Anita K. Jones
Kenneth H. Olsen
Wm. A. Wulf

Section 7

C. Kumar N. Patel

Section 8

Robert A. Pritzker

Section 11

Richard M. Morrow

Section 12

George M.C. Fisher
Simon Ramo

$20,000 to $99,999

Section 1

William A. Anders
Holt Ashley
Daniel J. Fink
Richard L. Garwin
James N. Krebs
Jack S. Parker
Allen E. Puckett
Eberhardt Rechtin
Brian H. Rowe
Robert C. Seamans, Jr.
H. Guyford Stever
Sheila E. Widnall

Section 2

Dane A. Miller
George B. Rathmann

Section 3

W. Kenneth Davis
Robert C. Forney
Gerald D. Laubach
Michael P. Ramage
Warren G. Schlinger

Section 4

Edgar J. Garbarini
Charles J. Pankow
Ivan M. Viest

Section 5

C. Gordon Bell
Erich Bloch
Lewis M. Branscomb

Section 6

William F. Allen, Jr.
E. Linn Draper, Jr.
Harold K. Forsen
John W. Landis

Section 7

Kenneth G. McKay
Morris Tanenbaum
Gary L. Tooker

Section 8

Robert A. Charpie
W. Dale Compton
Donald N. Frey
Trevor O. Jones
Charles E. Reed
Henry M. Rowan

Section 10

Robert J. Eaton
Simon Ostrach

Section 11

Thomas D. Barrow

Section 12

William W. Lang
Robert M. White

Rosette Society

Members and friends who contributed $5,000 or more to the National Academies in 2001

Section 1

Holt Ashley
Norman R. Augustine
Daniel J. Fink
Robert J. Hermann
Thomas V. Jones
Ruben F. Mettler
George E. Mueller
Jack S. Parker
Allen E. Puckett
Eberhardt Rechtin
Brian H. Rowe
H. Guyford Stever
Peter B. Teets
Robert H. Wertheim
Sheila E. Widnall
Edward Woll

Section 2

Dane A. Miller
Van C. Mow
Leo J. Thomas

Section 3

William L. Friend
Gerald D. Laubach
Michael P. Ramage
Warren G. Schlinger
Arnold F. Stancell

Section 4

Stephen D. Bechtel, Jr.
Harry E. Bovay, Jr.
Charles J. Pankow

Section 5

John A. Armstrong
Lewis M. Branscomb
Gerald P. Dineen
Charles M. Geschke
Anita K. Jones
Robert E. Kahn
Wm. A. Wulf

* Recently deceased

Section 6

William F. Allen, Jr.
E. Linn Draper, Jr.
John W. Landis

Section 7

Bernard M. Gordon
Donald R. Scifres
Gary L. Tooker

Section 8

Jordan J. Baruch
Robert A. Charpie
Robert A. Pritzker
Henry M. Rowan

Section 9

George A. Roberts
Dale F. Stein

Section 10

David Japikse

Section 11

Richard M. Morrow

Section 12

George M.C. Fisher
Samuel C. Florman

Charter Society

Members and friends who contributed between $1,000 and $4,999 to the National Academies in 2001

Section 1

Malcolm J. Abzug
Laurence J. Adams
Richard E. Adams
Oliver C. Boileau
James R. Burnett
Joseph V. Charyk
Hsien K. Cheng
Steven D. Dorfman
David R. Heebner
James N. Krebs
Hans W. Liepmann
Alan M. Lovelace
John L. McLucas
Norman F. Parker
Bradford W. Parkinson
Courtland D. Perkins
Theodore H.H. Pian
Robert C. Seamans, Jr.

Section 2

Edmund Y.S. Chao
Robert M. Nerem
George B. Rathmann
Hardy W. Trolander
Daniel I. C. Wang

Section 3

Andreas Acrivos
Charles R. Cutler
Robert C. Forney
Lester C. Krogh
Gerald D. Laubach
John P. Longwell
James F. Mathis
Walter L. Robb
William B. Russel
John J. Wise

Section 4

Clyde N. Baker, Jr.
Paul H. Gilbert
Delon Hampton
Theodore C. Kennedy
Charles C. Ladd
Thomas S. Maddock
James K. Mitchell
Norman A. Nadel
Richard J. Robbins
Alan M. Voorhees

Section 5

Paul Baran
Barry W. Boehm
Ruth M. Davis
Robert F. Sproull
Willis H. Ware

Section 6

Roy H. Beaton
Philip R. Clark
Harold K. Forsen
John G. Kassakian
Chauncey Starr
Henry E. Stone
Willis S. White, Jr.

Section 7

Frederick T. Andrews
David K. Barton
John M. Cioffi
Malcolm R. Currie
C. Chapin Cutler
Delores M. Etter
Thomas E. Everhart
G. David Forney, Jr.
Joseph W. Goodman
Paul E. Gray
Hermann K. Gummel
David A. Hodges
Thomas Kailath
James U. Lemke
John G. Linvill
James G. McGroddy
William J. Perry
Dennis J. Picard
Joseph E. Rowe
William G. Shepherd
Raymond S. Stata
Gunter Stein
Andrew J. Viterbi
Paul K. Weimer
Eugene Wong

Section 8

Paul A. Allaire
Donald C. Burnham
W. Dale Compton
Lee L. Davenport
Michael Field
Louis V. Gerstner, Jr.
James F. Lardner
William L. Maxwell
Donald E. Procknow
Linda S. Sanford
Maxine L. Savitz

Section 9

Craig R. Barrett
Lance A. Davis
Raymond F. Decker
Mary L. Good
Doris Kuhlmann-Wilsdorf
Frank W. Luerssen
Robert D. Maurer
Rustum Roy
Richard P. Simmons
Johannes Weertman
Julia R. Weertman
Albert R.C. Westwood

Section 10

Francois J. Castaing
Stephen H. Crandall
Edward E. Hagenlocker
Kenneth E. Haughton
Yao Tzu Li
Frederick F. Ling
Simon Ostrach
Donald E. Petersen
Frank E. Pickering
Bernard I. Robertson

Section 11

Thomas D. Barrow
Harry M. Conger
Thomas V. Falkie
Douglas W. Fuerstenau
William A. Griffith
Michel T. Halbouty
G. Frank Joklik
Jack E. Little
John Neerhout, Jr.
Franklin M. Orr, Jr.
Robert M. Sneider
Richard J. Stegemeier
John E. Swearingen

Section 12

Clarence R. Allen
Harold Brown
James J. Duderstadt
Dean Kamen
Ronald K. Leonard
John R. Moore
William F. Powers
Simon Ramo
Ernest T. Smerdon

Friends

Richard Atkinson
Kristine Bueche
Robert W. Galvin
James F. Hichman
Louise Stever

Other Individual Donors

Members and friends who contributed up to $999 to the National Academies in 2001

Section 1

Lew Allen, Jr.
Neil A. Armstrong
Irving L. Ashkenas
Seymour M. Bogdonoff
Alan C. Brown
Robert P. Caren
Earl H. Dowell
Robert E. Fischell
George J. Gleghorn
David G. Hoag
George W. Jeffs
Paul G. Kaminski
Don R. Kozlowski
Paul A. Libby
Peter W. Likins
Robert G. Loewy
Hans Mark
Russell G. Meyerand, Jr.
Angelo Miele
Joseph Miller
Rene H. Miller
Dale D. Myers
James G. O'Connor
William H. Pickering
Anatol Roshko
William R. Sears
Maurice E. Shank
Irving T. Waaland
John D. Warner
A. Thomas Young
Ben T. Zinn

Section 2

James B. Bassingthwaighte
J.H.U. Brown
Thomas F. Budinger
Lewis S. Edelheit
James Gillin
Adam Heller
Donald L. Johnson
Raphael Katzen
Robert Plonsey
John T. Watson
William D. Young

Section 3

John E. Anderson
John L. Anderson
P.L. Thibaut Brian
Nai Y. Chen
Morton M. Denn
James R. Fair
Robert C. Gunness
Sheldon E. Isakoff
Edward G. Jefferson
James R. Katzer
Riki Kobayashi
Johanna M.H. Levelt Sengers
Edward A. Mason
Walter G. May
Alfred Saffer
William R. Schowalter
Shirley E. Schwartz
Reuel Shinnar
Charles R. Wilke

Section 4

David P. Billington
Wilson V. Binger
Jack E. Buffington
George Bugliarello
L.G. Byrd
Jack V. Christiansen
Frederick J. Clarke
John L. Cleasby
G. Wayne Clough
Richard A. Conway
Don U. Deere
Albert A. Dorman
Carroll H. Dunn
John W. Fisher
Gerard F. Fox
E. Montford Fucik
Theodore V. Galambos
Ben C. Gerwick, Jr.
William J. Hall
Donald G. Iselin
Jeremy Isenberg
Wilfred D. Iwan
Robert B. Jansen
Paul C. Jennings
James O. Jirsa
Herbert S. Levinson
Robert C. Marini
Bryant Mather
Hudson Matlock
Charles C. Noble
Daniel A. Okun
Charles R. O'Melia
Karl S. Pister
Jerome L. Sackman
Reuben Samuels
Henry G. Schwartz, Jr.
Hsieh W. Shen
Franklin F. Snyder
Kenneth H. Stokoe II
James M. Symons
Robert V. Whitman

Section 5

Fernando J. Corbato
Edward A. Feigenbaum
Robert S. Hahn
Aravind K. Joshi
Barbara H. Liskov
Joel Moses
John R. Rice
Mischa Schwartz
Steven J. Wallach

Section 6

John G. Anderson
David H. Archer
Wm. H. Arnold
John W. Batchelor
Manson Benedict
W. Spencer Bloor
James D. Callen
Frederick J. Ellert
Ralph S. Gens
Charles H. Holley
Richard T. Lahey, Jr.
Thomas H. Lee*
Ludwig F. Lischer
Harry Mandil
James J. Markowsky
Warren F. Miller, Jr.
Peter Murray
Cordell Reed
Neil E. Todreas
Alvin W. Trivelpiece
Gregory S. Vassell
John J. Vithayathil
Harvey A. Wagner
J. Ernest Wilkins, Jr.
Bertram Wolfe

Section 7

Franklin H. Blecher
Esther M. Conwell
Douglass D. Crombie
Nicholas M. Donofrio
Irwin Dorros
Dean E. Eastman
Peter Elias*
Alan B. Fowler
Charles A. Fowler
Elmer G. Gilbert
Jerrier A. Haddad
Robert C. Hansen
David C. Hogg
Amos E. Joel, Jr.
Howard S. Jones, Jr.
Angel G. Jordan
Ivan P. Kaminow
Jack S. Kilby
Humboldt W. Leverenz
Ralph A. Logan
John C. McDonald
Kenneth G. McKay
Alan L. McWhorter
David Middleton
James J. Mikulski
Albert Narath
Marshall I. Nathan
Jacques I. Pankove
R. Fabian W. Pease
Robert H. Rediker
Walter A. Rosenblith
Steven B. Sample
Roland W. Schmitt
William F. Schreiber
Freeman D. Shepherd
Arnold H. Silver
Jack M. Sipress
Simon M. Sze

* Recently deceased

* Recently deceased

Lewis M. Terman
Charles H. Townes
Max T. Weiss
Irwin Welber
John R. Whinnery

Section 8

Jack L. Blumenthal
Geoffrey Boothroyd
Don B. Chaffin
Robert P. Clagett
Ralph L. Disney
John S. Foster, Jr.
James Hillier
Joseph M. Juran
Eugene S. Meieran
M. Eugene Merchant
Gerald Nadler
George L. Nemhauser
Joseph H. Newman
F. Stan Settles
James M. Tien
Paul E. Torgersen
Howard S. Turner
William L. Wearly
Edgar S. Woolard, Jr.

Section 9

Hubert I. Aaronson
John C. Angus
Donald J. Blickwede
Harvey Brooks
Harry G. Drickamer
Edith M. Flanigen
Norman A. Gjostein
Julius J. Harwood
Siegfried S. Hecker
John P. Hirth
William J. Koros
Alan Lawley
William J. MacKnight
David W. McCall
Bruce S. Old
Harold W. Paxton
Alan W. Pense
R. Byron Pipes
William R. Prindle
Nathan E. Promisel
Rangaswamy Srinivasan
Edgar A. Starke, Jr.
Robert H. Wagoner
Robert M. White

Section 10

H. Norman Abramson
Ronald J. Adrian
William G. Agnew
Charles A. Amann
Louis F. Coffin, Jr.
James W. Dally
George J. Dvorak
Fazil Erdogan
Nancy D. Fitzroy
Ronald L. Geer
Werner Goldsmith
William A. Gross
Carl G. Langner
Robert W. Mann
Roberta J. Nichols
Ronald F. Probstein
Allen F. Rhodes
Jerome G. Rivard
Warren M. Rohsenow
Ascher H. Shapiro
Peter G. Simpkins
Beno Sternlicht
Charles E. Taylor
Charles M. Vest
Raymond Viskanta

Section 11

Frank F. Aplan
Grigory I. Barenblatt
Robert F. Bauer
Robert R. Beebe
Lawrence B. Curtis
George J. Hirasaki
William C. Maurer
Thomas K. Perkins
Henry H. Rachford, Jr.
Robert J. Weimer

Section 12

David Atlas
Ken Austin
Arthur B. Baggeroer
Floyd Dunn
Helen T. Edwards
Robert A. Frosch
John H. Gibbons
Carl W. Hall
Howard R. Hart, Jr.
Eugenia Kalnay
Max A. Kohler
William W. Lang
Robert C. Lanphier III
Louis J. Lanzerotti
Margaret A. LeMone
Christopher L. Magee
Duncan T. Moore
Richard K. Moore
Stuart O. Nelson
Wesley L. Nyborg
Frank L. Parker
J. Randolph Paulling
Emil Pfender
Owen M. Phillips
Robert J. Serafin
Herman E. Sheets
Charles P. Spoelhoef
Richard G. Strauch
Gerald F. Tape
Valerian I. Tatarskii
Wilford F. Weeks
Robert M. White
David A. Woolhiser

Friends

Matthew Scott Cottle

Corporations, Foundations, and Other Organizations

American Electric Power Company, Inc.
AT&T Corporation
AT&T Foundation
Elizabeth and Stephen D. Bechtel, Jr., Foundation
Berwind Corporation
The Boeing Company
The Buffalo News
Concepts NREC, Inc.
Consolidated Edison Company of New York, Inc.
Cummins, Inc.
DaimlerChrysler Corporation
Delphi Automotive Systems
The Dow Chemical Company
E.I. du Pont de Nemours & Company
Duke Energy Corporation
Eastman Kodak Company
GE Fund
General Electric Company
General Motors Corporation
Japan Science and Technology Corporation
Lockheed Martin Corporation
Lucent Technologies, Inc.
The Marmon Group, Inc.
Microsoft Corporation
Motorola Foundation
Ohio University
Phillips Petroleum Company
Raytheon Company
Stratford Foundation
The Teagle Foundation, Inc.
Texas Utilities Company
TRW Inc.
United Technologies Corporation
Verizon Foundation
Xerox Corporation

The Safety of Our Water Systems

Excerpts from Testimony before the House Science Committee

Richard G. Luthy

Richard G. Luthy is a member of the NAE, the Silas H. Palmer Professor of Civil and Environmental Engineering at Stanford University, and chair of the National Research Council Water Science and Technology Board.

Since the sad events of September 11, we now question the vulnerability of our water systems to deliberate attack or sabotage. In the past, the vulnerability of our water systems to natural disasters received greater attention than vulnerability to deliberate acts. Our vulnerability concerns are compounded by the fact that many components of our water systems are aging and in need of repair, replacement, or upgrading. This is not a new state of affairs, but in the context of September 11, we are looking at the infrastructure of our water systems in a new light and thinking about how to protect them from intentional acts. The fundamental mission of water systems is to protect human health and ensure economic well-being. So despite recent events, we should not act precipitously. We must carefully consider new approaches to ensure the security of our water systems and, at the same time, to enhance their reliability and capability. Some of the key issues that need to be addressed are outlined below.

What elements of the water system are most vulnerable to physical damage, and how can we protect them? Dams and aqueducts and pumping stations that capture and convey water over long distances are especially vulnerable to physical damage. But even water supplies taken from rivers or lakes may be vulnerable if intakes are damaged. The control of access to critical components of water supply systems is likely to be much different for systems located in parks and public places than for systems in remote areas. In the last 20 years, we've fenced and locked facilities and covered reservoirs, but we will need more than that to prevent intentional acts. Some aqueducts are hundreds of miles long, and protecting them will be especially challenging. Our water supply systems have been designed to withstand natural disasters, and in-place systems for monitoring and responding to natural disasters could also serve as platforms for intrusion sensors and quick responses to intentional damage. The distribution system will be more difficult to secure. Although it potentially affects a smaller population, fear and anxiety can be caused even without mass exposure.

What chemicals, biological agents, or toxins would do the most to harm human health and be most disruptive? What points in the water supply, water treatment, and water distribution system are most vulnerable to the release of such agents? Because of the very large volumes of water being handled, many believe that truckload quantities of toxic chemicals would be necessary to cause harm. However, small quantities of toxic chemicals, even if not directly harmful, could cause panic and great economic disruption. Who would want to consume water to which low levels of lead or cyanide had been added? Biological agents, and especially their toxins, could be harmful at very low levels. Fewer than 10 spores or protozoan oocysts of some pathogens could cause infection; thus, small volumes of these agents in concentrated form could contaminate very large volumes of unfiltered water.

Surface water systems and systems that rely on groundwater, especially water from carbonate or other aquifers in which the water residence times are relatively short, are all vulnerable. Elevated portions of distribution systems, as well as pressurized conduits without backflow valves are vulnerable to the introduction of chemical or biological agents. Even a nontoxic substance could cause fear and anxiety if it caused a taste or odor.

How can we detect chemical or biological agents in the water supply system in time to take corrective action? We need better monitoring to provide an early warning of the presence of chemical or biological agents in the water supply. Water supplies are monitored routinely for a small number of contaminants and much less frequently for a large number of contaminants. However, conventional laboratory methods are time consuming and require skilled analysts. Therefore, problems arising from intentional acts might not be detected until chemical or biological agents had entered a treatment plant, or worse, a

distribution system (some large cities, notably San Francisco and New York City, have no treatment other than disinfection).

Much can be done to improve this situation. Most analytical equipment is highly automated and could probably be made more autonomous with new technologies. The chemical industry and some of the national laboratories are developing "chemical analysis on a chip" for hand-held, portable, chemical analysis systems and "canary on a chip" for detecting hazardous compounds in the workplace. With modifications, these systems might be used for the routine monitoring of water supplies for a broad spectrum of compounds, both known and unknown. With innovations in immunoassays and nanotechnologies, we could provide rapid screening for chemical and biological agents. But all of these technologies need much more development to be free from interference in natural settings. In addition, we should make use of time-tested methods, like increased chlorine demand, taste and odor, turbidity, and other measures, which are useful surrogate indicators that could be used in conjunction with new procedures.

How can water supply system operations be reconfigured to increase the interconnectedness of water supplies and potable water distribution systems? Interconnectedness is provided by conduits by which water can be transferred from one supply system to another. If one component of the water supply system is lost, other water supplies could be put on line to transfer water through standby conduits. Similarly, water distribution systems could be interconnected so that one locality could help another under emergency conditions. Mutual aid pacts could be made for water supplies, laboratory resources, operating assistance, and repair response.

This systems approach, often called regionalization, requires cooperation on a regional (often watershed) basis. Historically, because the water supply industry is fragmented, not much attention has been paid to designing for interconnectedness, except after the fact in cases of chemical spills or natural disasters. Greater interconnectedness would lead to greater stability and flexibility; systems with standby networks are less vulnerable to upset than monolithic entities. If a local water supply system were sabotaged, alternative water supplies could be brought in while the damaged system was flushed or repaired.

In the arid west, separate water supply systems are in place for agriculture and domestic use. Because so much more water is used for agriculture than by municipalities, the agricultural water supply or groundwater systems could be interconnected with domestic systems to augment the domestic supply in an emergency. Many questions, both technical and institutional, would have to be answered.

What changes in system operations or new technologies could protect against chemical or biological agents? We must think about new ways of supplying and treating water. Examples include the installation of robust standby treatment systems, for which we will need new technologies and augmented conventional technologies. Fortunately, advances in membrane, sorptive, and oxidative technologies can be brought to bear. For water reuse, a fundamental design paradigm is to install multiple barriers to provide safeguards in converting wastewater to potable water. These systems do not depend on one process but on several processes in a train that provide backup protection. We could extend the multiple barrier concept to create a series of hurdles to help us cope with chemical and biological agents. These barriers could be extended from the water treatment plant to include the distribution system and the point of use. Multiple barriers, such as storage capacity, enhanced treatment systems, and mutual aid, would allow the means and time to address a problem.

Are our water supply systems vulnerable to cyber attack? Historically, concerns about the safety of water supply systems have been focused on natural phenomena. However, today almost every component of water supply systems is highly automated, including the electronic control of water pumping and storage, control of water treatment operations, and regulation of water transmission. Although these operations are backed up by manual controls, great damage could be done if the automated control or the electric power for these systems were lost for a period of time due to cyber attack. Electronic security and emergency power backup capabilities will require careful analysis and possible reengineering.

Top priority should be given to protecting physical storage structures that serve large populations and that would be very difficult to replace, to ensuring water quality through better monitoring and new treatments, and to incorporating the concept of multiple barriers. All of these are crosscutting issues among disciplines and institutions. Designing effective solutions to key problems will require broad-based

studies that include university and government research establishments, professional organizations, practitioners, operators, and advice from groups like the National Research Council. Considering the range of threats to our nation's water supply, treatment, and distribution systems, a $50 million program annually for several years would be a minimum for engineering analysis and problem solving, scientific development, and reevaluation of water policies. New research programs must be organized and rigorously administered, including an independent peer review process, to ensure that the best research is pursued and the best results are obtained. The needs are too great for us to do otherwise.

In Memoriam

THEODORE A. BURTIS, 79, retired chairman, Sun Company, Inc., died on November 7, 2001. Mr. Burtis was elected to the NAE in 1984 for his contributions to the development of moving-bed catalyst systems and the management of large-scale energy programs.

PETER ELIAS, 78, Webster Professor of Electrical Engineering, emeritus, and senior lecturer, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, died on 7 December 2001. Dr. Elias was elected to the NAE in 1979 for pioneering work in the field of information theory and leadership in electrical engineering education.

WILLIAM H. HUGGINS, 82, professor emeritus, Johns Hopkins University, died on August 11, 2001. Dr. Huggins was elected to the NAE in 1970 for his contributions to electrical and biomedical engineering through radar and systems research, publications, and pedagogical innovation.

GEORGE R. JASNY, 77, retired vice president, Technical Operations, Martin Marietta Energy Systems, Inc., died on November 30, 2001. Mr. Jasny was elected to the NAE in 1983 for significant contributions to national defense, advances in uranium enrichment, and energy development through the effective technical management of complex engineering programs.

Symposium and Workshop: Technologies for Controlling CO_2 Emissions

The Kyoto Accords would require that the United States reduce its emissions of carbon dioxide (CO_2) to below 1990 levels, which would require substantial reductions in energy consumption. Because of concerns about the economic effects of meeting this requirement, the United States decided not to become a signatory to the treaty. To address these concerns, the NAE will hold a symposium and workshop, April 23–25, 2002, on current and emerging technologies that could help reduce CO_2 emissions or even remove CO_2 from the atmosphere. On the first day, speakers in the forefront of the field will cover the global and political context of CO_2 reduction technologies, the economics of reducing CO_2 emissions, and the potential uses of new and emerging technologies for developing nations. The workshop will include breakout sessions to examine alternatives in more detail. For more information contact: Dr. Brendan P. Dooher (bdooher@nae.edu; 202-334-1251).

Calendar of Meetings and Events

January 15	Governing Board Executive Committee
January 17	Symposium on Mandate for Technological Literacy
January 23–24	Forum on Diversity in the Engineering Workforce *Irvine, California*
January 24–25	Committee on Diversity in the Engineering Workforce *Irvine, California*
January 28	Engineering Education Research Retreat
January 29	Finance and Budget Committee
February 4–5	NRC Governing Board *Irvine, California*
February 5	NAS/NAE Council Dinner *Irvine, California*
February 6	NAS/NAE Officers Breakfast NAS/NAE Council Meeting *Irvine, California*
February 6–7	NAE Council Meeting *Irvine, California*
February 8	NAE National Meeting Frontiers of Engineering: Gilbreth Lecture Series *Irvine, California*
February 11–12	Committee on Diversity in the Engineering Workforce
February 12	Governing Board Executive Committee NAE/ASEE Engineering Deans Colloquium
February 19	2002 NAE Awards Dinner and Presentation Ceremony *Union Station, Washington, D.C.*
February 22	NAE Regional Meeting Sensor Networks for Health Care, the Environment, and Homeland Defense *University of California, San Diego*
March 1–3	U.S. Frontiers of Engineering Symposium (rescheduled from September 13–15, 2001) *Irvine, California*
March 5	NAE Regional Meeting Engineering a New Century *University of Texas at Austin*
March 12	Governing Board Executive Committee
March 18	NAE Regional Meeting Secure Electricity for Twenty-First Century America *University of Wisconsin-Madison*
April 9	Governing Board Executive Committee
April 12	NAE Regional Meeting Frontiers in e-Learning *University of Arizona, Tucson*
April 12–13	STS and Globalization Conference
April 23–25	Complements to Kyoto: Technologies for Controlling CO_2 Emissions
April 27–30	2002 NAS Annual Meeting
April 30	Finance and Budget Committee Conference Call
May 22	NAE Regional Meeting Engineering Thin Films at the Nanoscale *North Carolina State University, Raleigh*

All meetings are held in the National Academies Building, Washington, D.C., unless otherwise noted.

NAE Newsmakers

Anil K. Chopra, Johnson Professor of Civil Engineering, University of California at Berkeley, was awarded the **2001 ASCE Norman Medal** for "Evaluation of NSP to Estimate Seismic Deformation: SDF Systems," which was judged the best paper published in an ASCE journal.

James W. Cooley, a retired researcher, IBM Thomas J. Watson Research Center, was named the recipient of the **2002 IEEE Jack S. Kilby Signal Processing Medal**. Dr. Cooley was recognized for his pioneering work on the fast Fourier transformation (FFT) algorithm.

Douglas W. Fuerstenau, professor in the Graduate School, Department of Materials Science and Engineering, University of California, Berkeley, was recently awarded an honorary degree of **Doctor of Engineering** (Tekn. Dr. [h.c.]) by Luleå University of Technology in Sweden. He received this distinction for his unique achievements in research and development in mineral engineering over a period of many years and for inspiring researchers in the field.

Nick Holonyak, John Bardeen Chair Professor of Electrical and Computer Engineering and Physics, University of Illinois, received the 2001 **Frederic Ives Medal/Jarus W. Quinn Endowment**, the Optical Society of America's most prestigious honor.

James Padilla, group vice president, Global Manufacturing, Ford Motor Company, received the **Brillante Award**. Mr. Padilla was recognized for exceptional contributions to the Hispanic community by individuals, corporations, and universities.

Ponisseril Somasundaran, director, NSF/IUCR Center for Surfactants and La Von Duddleson Krumb Professor, Columbia University, was the keynote speaker and honorary chair of the International Symposium on Nanomaterials and Technology held in Beijing, China, in July 2001. During his stay, he was invited to meet President Jiang Zemin.

On November 5, 2001, **Jack H. Westbrook**, president and principal consultant, Brookline Technologies, received the **Albert Sauveur Achievement Award** for 2001 from ASM International. Dr. Westbrook was honored for his "contributions calling attention to intermetallic compounds as a new class of engineered materials and advancing scientific understanding of their behavior, particularly their mechanical properties, constitution, and defect structures."

C.P. Wong, Regents' Professor of Materials Science and Engineering, Georgia Institute of Technology, received the 2001 IEEE Educational Activities Board **Meritorious Achievement Award in Continuing Education**. Dr. Wong was recognized for exemplary and sustained contributions to continuing education in polymer materials for electronics packaging and interconnections worldwide.

Dr. Robert Cherry Joins the NAE as Fellow

Robert Cherry

Dr. Robert Cherry began a yearlong fellowship with the NAE Program Office in early December. He comes to the NAE from the Idaho National Engineering and Environmental Laboratory (INEEL), where he conducted research on methane hydrates, hydrogen production from diesel fuel, and biological conversions for the treatment of several types of industrial waste.

Prior to that, Dr. Cherry was on the faculty at Duke University and worked for a number of years in industry with Arco Chemical Company and Exxon Research and Engineering Company. He holds a B.S. and M.S. from Massachusetts Institute of Technology and a Ph.D. from Rice University, all in chemical engineering.

At the NAE, Dr. Cherry will develop and direct a project to explore the environmental and global consequences of using bioenergy as an alternative to fossil energy.

Tom Ridge, Terrorism Experts Meet with News Executives

Wm. A. Wulf, Governor Tom Ridge, and Jack Cox

On December 6, 2001, engineers, scientists, and researchers gathered in Washington, D.C., to brief news executives on the targets and manifestations of terrorism. The purpose of the gathering, "Terror and Homeland Defense: Bringing the Stories Home," was to promote accurate and effective reporting on terrorism-related issues. Governor Tom Ridge, director of the White House Office of Homeland Security, was the keynote speaker. The conference was cosponsored by the NAE and the Foundation for American Communications (FACS).

Anthony Cordesman, Arleigh Burke Chair and Senior Fellow, Strategic Assessment, of the Center for Strategic and International Studies, began the conference with a sobering look at the history and motivations of terrorists. Cordesman said U.S. military, law enforcement, and emergency response teams must be prepared to defend against asymmetric attacks but must also acknowledge that this problem can never be completely eradicated.

NAE President **Wm. A. Wulf** then described the vast array of targets, weapons, and delivery systems available to terrorists. He concluded that once the most likely attack scenarios had been identified, the nation could effectively prepare for the most destructive ones. The NAE is sponsoring a year-long study headed by **Alvin Trivelpiece**, Ph.D., NAE member, and former director of Oak Ridge National Laboratory, to analyze the risks and complex consequences of various means of attack on critical infrastructures.

Baruch Fischhoff, Ph.D., professor of engineering, Department of Social and Decisions Sciences, Carnegie Mellon University, showed that assessing the real risks of terrorism will require examining complex, interrelated events. His psychological research has shown that no matter how disturbing the situation, the public responds better to the truth than to a lack of information.

Governor Tom Ridge emphasized the importance of technology in coordinating intelligence, law enforcement, and medical activities. Governor Ridge stated, "The best way to protect America is to push the perimeter as far out as possible and to provide as much time and distance as possible to detect, disrupt, and prevent."

The afternoon was devoted to sessions on different means of terrorist attack and their relative risks. Margaret Hamburg, M.D., vice president for biological programs at the Nuclear Threat Initiative and former New York City health commissioner, provided background on anthrax, smallpox, and the preparedness of the medical community for bioweapons attack. The media, she said, are in a unique position to investigate and publicize the readiness of public health agencies and other first responders in their local communities.

According to NAE member **Richard Garwin**, Ph.D., Philip D. Reed Senior Fellow for Science and Technology at the Council on Foreign Relations in New York, the most likely form of nuclear attack would be a "dirty bomb." Although the number of casualties from such an attack would be low, especially compared to the number from a biological attack, it would generate a high level of persistent fear.

Jeffrey Hunker, Ph.D., dean, H. John Heinz III School of Public Policy and Management, Carnegie Mellon University, described cyberattacks, cybersecurity, and the looming threat of cyberwar. He pointed out that because no one really understands how interconnected our systems are, it is nearly impossible at this point to predict how we would be affected if one system (e.g., an energy grid) were attacked.

NAE member **Jeremy Isenberg**, Ph.D., president and CEO of Weidlinger Associates in New York, showed how computer models can now accurately predict the effects of blasts on buildings. Isenberg also described structural defenses against bombs and some of the blast mitigation measures available to engineers, such as wrapping concrete columns in steel and coating windows with a film to prevent flying shards. Most buildings are designed to meet budget requirements, not to withstand explosions.

As the day ended, the 50 attendees engaged the speakers in a lively panel discussion on the particulars of how the media could identify and cover important terrorism-related issues. As the conference showed, engineers can contribute vital expertise to help the media inform the public.

National Research Council Update

Military Know-how Can Help Protect Civilian Buildings from Attacks

The U.S. Department of Defense (DOD) Defense Threat Reduction Agency (DTRA) Blast Mitigation for Structures Program was established by Congress in 1997 to identify and implement engineering methods that could protect lives by reducing bomb damage to buildings. In a review of the program, the National Research Council recommends research activities and methods of transferring the findings to the building industry.

The study recommends that DTRA share the results of its research and testing program with civilian engineers, architects, and builders, as well as with other federal agencies. To date, DOD's efforts have been focused on protecting the military community and buildings. The report calls on DTRA to take the lead in communicating research results on blast effects and innovative techniques for protecting against them. The report also urges the federal government to set up rapid-response teams to collect medical information about injuries, illnesses, and casualties that result from bombing attacks and to establish a database for storing and analyzing the data.

Because it may be very costly to construct or retrofit buildings to withstand explosions, the committee suggests that blast-resistant features be part of a larger strategy to protect buildings from a variety of hazards. Because every building has distinct purposes, design and site considerations, and budgets, hazard mitigation measures should be tailored for each building. The arrangement of nonstructural features should also be taken into consideration.

NAE members on this committee were **Mete A. Sozen**, Purdue University; **W. Gene Corley**, Construction Technology Laboratories, Inc.; **Robert P. Kennedy**, RPK Structural Mechanics Consulting; **Eugene Sevin**, independent consultant; and **Charles H. Thornton**, Thornton-Tomasetti Engineers. The full text of the report, *Protecting People and Buildings from Terrorism: Technology Transfer for Blast-Effects Mitigation*, is available online at <*http://www.nap.edu/catalog/10230.html*>.

Promoting Residential Broadband Internet Access

A recent report by the Committee on Broadband Last Mile Technology recommends that the federal government support new initiatives to bring broadband Internet access to U.S. homes rather than pursuing premature policies that could inhibit the market. The committee concludes that once the market takes shape, policy makers will have a better understanding of what forms of government intervention, if any, will be necessary. Broadband promises to provide consumers with advanced capabilities, such as electronic health care applications, real-time participation in meetings via computers, and more interconnected devices in the home.

A central finding of the report is that local efforts to bring broadband services to more homes should be strongly encouraged. Local governments could encourage businesses to enter the market by forming partnerships with them to install fiber-optic cables. Local public agencies could

work with communities and area institutions to stimulate demand for, and the use of, broadband.

The report favors competition among facilities-based service providers for the long term for several reasons. A competitive market would require less government regulation than mandated unbundling, would promote diversity in the kinds of services offered, would avoid the technical problems and other problems associated with the unbundling of copper lines, and would reduce the disincentives for established providers to innovate and expand their services.

NAE members on the committee were **Nikil Jayant** (chair), Georgia Institute of Technology and Georgia Tech Broadband Institute; **John M. Cioffi**, Stanford University; **David D. Clark**, Massachusetts Institute of Technology; and **Paul E. Green, Jr.**, Tellabs, Inc. (retired). The full text of the report, *Broadband: Bringing Home the Bits*, is available online at <*http://www.nap.edu/catalog/10235.html?onpi_topnews_112901*>.

United States Bolsters Encryption Standards

A 1996 National Research Council report, *Cryptography's Role in Securing the Information Society*, concluded that the widespread use of cryptography would benefit the nation in many ways: by providing better protection from crime and terrorism for banking and telecommunications networks, by providing greater privacy for individuals, and by boosting the international competitiveness of U.S. companies. According to the U.S. Department of Commerce, tough federal encryption standards adopted in December 2001 will protect electronically transmitted government, financial, and personal data. The new standards, which are expected to be widely used in the private sector, will offer greater security for individual transactions, such as electronic cash withdrawals, e-mails, and online shopping.

NAE members **Samuel H. Fuller**, Analog Devices, Inc., and **Willis H. Ware**, RAND Corporation, were members of the study committee. The full text of the 1996 report is available at <*http://www.nap.edu/catalog/5131.html*>.

Correction

In the winter 2001 issue of *The Bridge*, an NRC report, *Analysis of Engineering Design Studies for Demilitarization of Assembled Chemical Weapons at Pueblo Chemical Depot*, was incorrectly attributed. The study was conducted by the Committee on Review and Analysis of Alternative Technologies for the Demilitarization of Assembled Chemical Weapons: Phase II. NAE members on the committee are **Sheldon E. Isakoff**, Engineering R&D Division, E.I. du Pont de Nemours & Company (retired); **Frederick J. Krambeck**, ExxonMobil Research and Engineering Company; and **Stanley I. Sandler**, University of Delaware.

Publications of Interest

The following reports have been published recently by the National Academy of Engineering or the National Research Council. Unless otherwise noted, all publications are for sale (prepaid) from the National Academy Press (NAP), 2101 Constitution Avenue, N.W., Lockbox 285, Washington, DC 20055. For more information or to place an order, contact NAP online at <*http://www.nap.edu*> or by phone at (800) 624-6242. *(Note: Prices quoted by NAP are subject to change without notice. Online orders receive a 20 percent discount. Please add $4.50 for shipping and handling for the first book and $0.95 for each additional book. Add applicable sales tax or GST if you live in CA, DC, FL, MD, MO, TX, or Canada.)*

Perspectives on the Department of Defense Global Emerging Infections Surveillance and Response System: A Program Review. Presidential Decision Directive NSTC-7 declared that national and international capabilities for the surveillance, prevention, and response to outbreaks of infectious diseases were inadequate to protect the health of U.S. citizens and called for a robust national policy to improve these capabilities. NSTC-7 directed many U.S. federal agencies, including the U.S. Department of Defense (DOD), to take action. In response, DOD established the global emerging infections surveillance and response system (GEIS) in 1997. In April 2000, the Institute of Medicine convened a committee to evaluate the progress of GEIS, which is still in the early stages of development. The committee concluded that GEIS is an appropriate DOD response to NSTC-7 and to the threat of emerging infectious diseases. With increased support, and some refinements, the program has the potential to meet, or even exceed, the requirements of NSTC-7. Paper, $36.25.

Review of the Future of the U.S. Aerospace Infrastructure and Aerospace Engineering Disciplines to Meet the Needs of the Air Force and the Department of Defense. This report recommends that an Air Force deputy chief of staff position be established with primary responsibility for overseeing all Air Force scientific and technical resources; the new deputy chief of staff would be the advocate for funding science and technology requirements and would ensure that adequate funding is budgeted annually. Other recommendations address the issues of technical personnel, expenditures and investments, the establishment of partnerships with industries and universities and their faculty members, and the reform of Civil Service rules for scientific and technical personnel. Paper, $18.00.

Review of the U.S. Department of Defense Air, Space, and Supporting Information Systems Science and Technology Program. This report recommends that the Air Force continue to: increase its investment in science and technology (S&T) to twice its FY01 level; take action to strengthen S&T representation and advocacy at the corporate policy and decision-making level of the Air Force; request that Congress extend the pilot program for revitalizing the service laboratories by at least three years; and work to enact targeted modifications of Civil Service rules that directly affect the quality of the S&T workforce. Paper, $18.00.

Technically Speaking: Why All Americans Need to Know More About Technology. Cell phones . . . air bags . . . genetically modified food . . . and the Internet are all emblems of modern life. Most people would be hard pressed to know how we would function without them. They would have even more trouble, however, explaining how they work. The United States is riding a whirlwind of technological change that has significant, far-reaching social, economic, and other impacts. It seems that the faster we embrace new technologies, however, the less we understand them. In this new, technology-dependent world, an understanding of the nature and implications of technology is a matter of responsible citizenship. *Technically Speaking: Why All Americans Need to Know More About Technology* provides a blueprint for bringing us all up to speed on the role of technology in our society, including the distinctions between technology and science and technological literacy and technical competence. The report provides an overview of the subject, highlights specific issues of concern, and three case studies—air bags, genetically modified foods, and the California energy crisis. Paper, $19.95.