Hardening critical infrastructure against terrorist attack may be one of the most challenging responsibilities of the homeland security mission. This year, we can expect policymakers and private infrastructure owners to ratchet up debate on how to best approach this massive task.

America is an open and technologically complex society with an almost unlimited number of potential targets and points of vulnerability. Examples of these that the U.S. Department of Homeland Security (DHS) has identified include more than 168,000 public water systems, 300,000 oil and gas production facilities, and 100 nuclear power plants. A White House assessment counted 2,800 electrical plants, 590,000 highway bridges, 66,000 chemical plants, 2 million miles of pipelines, and 1,800 federal reservoirs.

Making the task of hardening these and other facilities all the more difficult is the fact that the better a particular facility or system is protected, the more likely it is that attacks will be diverted to more vulnerable targets.

Moreover, hardening infrastructure to reduce the effects of an attack is only one of the goals of the DHS’ strategic plan. The others include raising public awareness of the threats, vulnerabilities, and potential impact of attacks; sharing intelligence among agencies to prevent attacks; and strengthening the nation’s ability to respond to, and quickly recover from, an attack.

Not surprisingly, these goals compete intensely for resources. Significantly, the congressional 9-11 Commission report included little reference to critical infrastructure protection. In part, this is because emergency management has historically focused on disaster preparedness and response rather than on prevention — the reason being that natural disasters are largely unavoidable. As a result, the complex agenda for hardening the nation’s infrastructure against attack is still in its early stages.

Response to attack has been focus of funding

In the last three years, the DHS and its predecessor agencies have spent more than $12.5 billion to strengthen state and local governments’ response to attacks. Most of this funding has gone to first responders such as police and fire departments. The current DHS budget includes an additional $3.6 billion for similar purposes.

Infrastructure protection has received far less attention, but there are signs that federal spending in this area may increase. The current DHS budget includes the agency’s first infrastructure protection grants — $200 million for specific facilities such as nuclear plants, dams, highways, railroads, or tunnels. However, these grants will only fund some high-visibility pilot projects, rather than constituting a comprehensive program.

In addition, the DHS has worked for nearly a year on its National Infrastructure Protection Plan (NIPP), the purpose of which is to help prioritize spending on infrastructure hardening. The plan will establish the framework and processes by which 17 infrastructure sectors will compete for resources with each other and with other homeland security objectives.

In addition, the NIPP will set the stage for addressing government’s role in dealing with the private sector, which owns 85 percent of the nation’s critical infrastructure. It will likely spark discussion about encouraging infrastructure protection initiatives in the private sector, through public funding, tax law changes, or regulatory changes.

Three key measures needed in national plan

To be a useful and credible guide to strategic decision-making for infrastructure protection, any national infrastructure protection plan must successfully address three basic issues:

First, it must be able to identify targets that, if attacked, would result in the largest loss of...
life or the gravest economic or social impact. From this perspective, not all facilities need protection to the same level — regardless of losses that owners of a particular system would suffer in an attack. Setting risk-based priorities may prove contentious, but with limited resources for protecting such vast infrastructure, it's a practical necessity.

Second, it must advance our understanding of the complex interdependencies among infrastructure systems. For instance, 2003’s electrical outages in the U.S. Northeast interrupted water supplies and cellular communications in cases where power backups fell short. Learning more about such interdependencies will help us prevent catastrophic cascading effects, build in redundancy, and reduce restoration and recovery time.

Finally, the plan must build on the work that has been done in the name of mitigating natural hazards. For instance, the American Lifelines Alliance (ALA) has worked with FEMA and the National Institute of Building Sciences on guidelines to assess the vulnerability of systems such as electric power, oil and gas, and water and wastewater, and has developed approaches to protect these systems from a variety of hazards.

Infrastructure owners may be more concerned about natural or accidental hazards, yet the steps they take against these threats can also protect against terrorist strikes. For example, putting transmission lines underground protects against wind, ice, and tree damage — and sabotage as well. Likewise, building fire resistance into tunnels lowers the risk of accidental fires, while at the same time making the tunnels less attractive targets for attack. The ALA brings together public and private infrastructure owners experienced in hazard mitigation, offering a forum for the discussion of infrastructure hardening.

Many questions remain about how to best protect critical infrastructure. But the first steps must include identifying the sectors and facilities that are not only at highest risk, but also present the most serious consequences if attacked, and allocating resources to these top-priority targets.

About Laurence W. Zensinger
Laurence W. Zensinger is vice president and director of homeland security for Dewberry, an architecture and engineering firm based in Fairfax, Va. He is a former homeland security and emergency management senior executive for the U.S. Department of Homeland Security’s Federal Emergency Management Agency (FEMA).

Zensinger most recently served as deputy director of FEMA’s Recovery Division, which provides disaster relief nationwide, including services and funding for infrastructure restoration. Following the Sept. 11, 2001, terrorist attacks, he helped direct major recovery issues including debris operations, environmental testing and cleanup, economic impact analysis, and the creation of a $4.5 billion funding package to rebuild lower Manhattan’s mass transit infrastructure.

Coming in the next BE Magazine
Highlights from the next issue of BE Magazine:

More information on BE Conference 2005
Profiles of outstanding projects from the BE Awards of Excellence
Landscape architect turned Peace Corps volunteer uses MicroStation to help build communities in Albania
How knowledge management helps Fluor compete globally
Survey of U.K. CAD managers suggests ways to work better
Highlights of an interview with Greg Bentley by Tom Sawyer, Engineering News-Record associate editor, information technology
Engineers Without Borders links professionals and students to aid developing nations
New study data demonstrating return on investment from Bentley ProjectWise

Submitting articles for Viewpoints
BE Magazine welcomes your thoughts and perspectives on any topic concerning architecture, engineering, construction, related technologies, or infrastructure in general.

The Viewpoints section is a place for your own commentaries or points of view. Company or professional news items will be considered for our news sections. Opinion pieces of 150 words or less will be considered for our Letters section.

Please do not send us completed articles. Instead, send a brief proposal outlining the article you would like to submit.

All submissions may be edited for length and clarity, and BE Magazine reserves the right to reject any submission. Please include contact information.

Send submissions to BEmagazine@be.org.