The 3rd International Conference on Structural Health Monitoring of Intelligent Infrastructure
Vancouver, British Columbia, Canada
November 13-16, 2007

THE CHALLENGE OF ECONOMICALLY BALANCING SECURITY AND MOBILITY NEEDS OF OUR NATION'S BRIDGE INFRASTRUCTURE

Harry A. Capers, Jr. PE, Corporate Bridge Engineer
Arora and Associates PC, USA

Narendra Khambhati, PE, Senior Vice President
Arora and Associates PC, USA

Abstract

After 9/11 many studies have been made to examine the protection of the highway infrastructure against terrorist attacks. Initial conclusions were that achieving security for the transportation system would be "difficult and costly but necessary." While it may be difficult and necessary, we need to find ways not to make it costly but rather a part of the normal design. Costs of addressing the aging infrastructure issue are already far outstripping resources available and as such, owners can ill afford adding to the bill. Designing for security must become a routine part of new design addressed along with all of the other extreme events and taking advantage of details already thee to address those loads.

For the existing inventory, owners need to assess vulnerabilities, rank assets, then apply detection, deterrence, denial, defense, reaction and recovery strategies to most efficiently respond to threats to our transportation system. One of the goals of terrorists is to significantly affect our way of life by attacking our economy. We need to find ways to minimize his ability to achieve this by attacking our transportation infrastructure. This paper outlines several efforts in this area, including opportunities and challenges still to come.

INTRODUCTION

It has been often said that September 11, 2001 drastically changed the world we live in. This has proven to be a very true statement and as we recovered from the national grief and frustration and moved to action, this became very true for the custodians of our nation's infrastructure.

Probably in a very typical response to a national threat owners and agencies began to take actions to secure their assets. A whole new "Homeland Security" industry seemed to come into being. Not unwisely, owners began to scan available knowledge to see what best practices were available for use in protecting their assets against this increased peril.

Blue Ribbon Panel

Early on one of the biggest challenges facing owners was determining what the threat to their asset was. Throughout the 1990's terrorist attacks around the world demonstrated the creativity and determination of terrorist organizations in their attacks against targets of interest to their leadership. Owners had a massive number of issues

that needed to be answered not the least of which was what national agency would assume the leadership role in developing security standards and where would the resources come from.

Reacting to the need the American Association of State Highway and Transportation Officials (AASHTO) in conjunction with the Federal Highway Administration (FHWA) initiated several activities to address this knowledge gap. One was the formation of a Blue Ribbon Panel (BRP) on Bridge and Tunnel Security. This panel, working through a National Cooperative Highway Research Program (NCHRP) Project 20-59(3) "FHWA/AASHTO Blue Ribbon Panel on Bridge and Tunnel Security" was charged with two tasks. These were first to provide direction for a national security-related policy to guide the owners/operators of highway infrastructure and second to develop short- and long-term strategies for improving the safety and security of the Nation's bridges and tunnels. While the group received many briefings on how to identify and clarify the issues, develop and evaluate potential solutions, and formulate and refine recommendations for improving bridge and tunnel security, it should be recognized that the material provided them was all open source material. That be as it may, the panel still was able to provide extremely valuable insights and recommendations from which to proceed.

The first significant conclusion of the panel was that the threat to our transportation system was real. The panel concluded, "The success and safety of the system (during several historical events), and perceived number of parallel routes does not mean that transportation system is invulnerable to significant disruption by terrorist attack."[1] In fact the transportation system in the United States was already straining to meet demand in many places and many obvious choke points exist at major bridge crossing points and tunnels.

The second major conclusion was that an attack upon a major bridge or tunnel could result in severe economic consequences and prove to be severely disruptive to regional and national economy. The panel concluded that the cost of replacement of a major river crossing and the economic loss to the economy was in $tens of billions based on estimates from recent earthquakes.

Having concluded the above the Blue Ribbon Panel made seven important recommendations to reduce the vulnerability of bridges and tunnels to terrorist attacks. The panel organized these recommendations into three areas: institutional, fiscal, and technical. The recommendations in the technical area were contingent on implementation of those in the fiscal and institutional areas.

Three Institutional Recommendations were made. The first recognized the importance of having FHWA, AASHTO, Transportation Security Administration (TSA), and other highway transportation stakeholders collaborate to ensure that assessment methodologies and security solutions meet stakeholder needs. The second suggested FHWA and AASHTO's role, in partnership with other organizations, in disseminating information about bridge and tunnel security and cost-effective countermeasures to decision-makers, facility owners/operators, designers, and elected officials. The final institutional recommendation was for FHWA to seek clarification on the legal responsibility of state Departments of Transportation (DOTs) and public transportation authorities to take action on conclusions drawn from vulnerability studies.

Two Fiscal Recommendations were made. First was that New Funding Sources for Bridge and Tunnel Security beyond and outside of current federal-aid highway funding sources. The second was that expenditures for cost-effective strategies for bridge security should be allowed using federal funding for critical structures without regard to deficiency as currently defined, as was done for seismic retrofitting or scour countermeasures. .

Finally two Technical Recommendations were made. The first of these was that security solutions should be "engineered" and that FHWA should be given the coordinate with TSA to prioritize critical bridges and tunnels and to administer fund allocation to responsible agencies to address security issues. The second recommendation recognized the fact that engineering standards do not exist for security of bridges and tunnels. This recommendation called for the development and validation of security technology initiatives through appropriate research and development (R&D).

The seven recommendations outlined above are the heart of the BRP's recommendations for security of bridge and tunnels In addition, specific technical recommendations including identifying critical bridges and tunnels, operational security measures, engineering and design approaches, and research and development agenda were included in the report.

Vulnerability Assessments
Another significant activity initiated by AASHTO and FHWA to address security needs of the transportation community was the development of the "Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection" again prepared under a NCHRP project, Project 20-07/Task 151B. The Guide was developed as a tool for owners to assess the vulnerabilities of their assets, to develop possible countermeasures to deter, detect, and delay threats, to estimate the capital and operating costs of such countermeasures; and improve security operational planning of the agencies.

The Guide was intended to be usable by a broad audience within transportation agencies. It includes guidance for the initial planning of a vulnerability assessment for senior officials, reference material for use by mid-level managers in preparing assessment plans and procedures, and examples for field personnel who will likely conduct the assessments of critical assets. It provides for the formation of multidisciplinary teams familiar with the agency and affected assets. It also identifies the types of resources typically required to conduct a vulnerability assessment, finally, the guide describes the three major phases of the assessment process – pre-assessment, assessment, and post-assessment. This six-step process is an integrated and iterative approach to vulnerability assessment of owner's critical assets. It should be noted that the process is "evergreen" and must be repeated as often as assumptions change.

OUR CHALLENGES

The Threat
Analysts conclude that Terrorists' pursuit of their long-term strategic objectives includes attacks on critical infrastructures and key assets. Terrorists target critical infrastructures to achieve three general types of effects. The first of these is to create physical destruction and disruption. They look for direct infrastructure effects by causing cascading disruption or arrest of the functions of the critical infrastructures or key assets through direct attacks on a critical node, system, or function. They might also seek indirect infrastructure effects through Cascading disruption and financial consequences for government, society, and economy through public- and private sector reactions to an attack. Another goal might be to attempt exploitation of elements of a particular infrastructure to disrupt or destroy another target

The second effect is to create a climate of fear, which is aided and abetted by an audience-hungry media. Terrorists hope that by causing mass casualties or destruction of a symbol of historic or cultural significance they will cause pressure to be exerted on leadership in favor of their goals.

The third effect they hope to achieve is to cause disruption of our every day business and to cause us to incur extra costs for security measures incurred to prevent terrorism. In accomplishing this terrorists have a direct impact on a society's way of life by drawing down on financial resources it otherwise would use for other purposes.

Terrorist objectives are presumed to be to cause political, economic and social disruption. Their preferred targets continue to be "soft" targets, such as business & tourist sites. Transportation assets in general have relatively low attractiveness as terrorist targets because of the relatively low potential for casualties. Transit and rail systems are more likely targets in the transportation sector as has been demonstrated by recent attacks in Madrid and London.

Major bridges and tunnels, spanning large rivers, bays, and mountains are assumed the most attractive terrorist targets within the transportation system. The loss or damage to many such structures could have negative impacts as they may have high symbolic value, can result in large financial burdens due to the response, recovery and replacement, and depending on the timing of the attack, could result in potentially large numbers of casualties.

Vulnerability Assessments
Very soon after the "Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection" became available and began to be used, the exercise revealed the first challenge for owners to overcome. The challenge was ensuring the assessment addressed all critical infrastructures that the bridges could affect just not the bridge. The bridge becomes significant because of the service it provides to an environment and as such it must be

looked at as a part of the environment in which it sits. Further it must be examined from a local, regional, state and national perspective. The vulnerability assessment process is what we refer to as “evergreen”, or never completed. As the threat changes, new technologies become available, strategies change or an assets significant change the assessment must be redone. For many agencies, this is a big challenge as the process is complex. This is certainly a major challenge for agencies.

Target, Weapon or Platform?

It is very important that a bridge needs to be considered not just as a target. While the bridge engineer may want to believe that the structure is the most important element in a setting, it must be looked at in the big picture. A span over a navigable waterway, railroad, major highway or other significant crossing might be used as a weapon to deny the use of the element it is crossing. A small structure over what would be an otherwise insignificant crossing could even have great significance if it’s loss or the loss of the facility it crossed prevented access to another asset that is the real target by first responders.

In many situations a bridge could also serve as the platform from which to launch an attack. Many of our crossings provide clear lines of sight to other critical features adjacent to their location. Identifying and properly assessing all of New Jersey’s critical infrastructure elements that might be affected by a bridge was proven to be an intense exercise.

Multidisciplinary Teams

Properly identifying and assembling assessment teams is also a challenging task. To perform a proper assessment requires assembling the proper Multidisciplinary teams.

These Multidisciplinary teams, consisting of groups of professionals from diverse disciplines, are key to success. They can promote coordination between agencies and infrastructure sectors to provide a "checks and balances" mechanism in the process. A good team can ensure that the interests and rights of all concerned parties are addressed. They can identify service gaps and breakdowns in coordination or communication of security plans between agencies or individuals. They also enhance the professional skills and knowledge of individual team members by providing a forum for learning more about the strategies, resources, and approaches used by other disciplines.

Each discipline has its own perspective, jargon, mandates, and resources. When professionals fail to understand these differences, it can create barriers, misunderstandings, or "turf" conflicts. On the other hand, when professionals learn about other disciplines' approaches, resources, and perspectives, it can greatly expand their repertoires of skills, increase the resources they can make available, and enhance their understanding of security issues facing other sectors. These teams can facilitate interagency coordination, resulting in a more comprehensive range of services, reducing the likelihood that something will "fall between the cracks", and cutting down on the overall risk to an asset. Agencies must make sure that they engage all of the possible stakeholders impacted by their assets in ranking assets, determining vulnerabilities and outlining countermeasures.

Jurisdiction

Overlapping jurisdiction and the ownership of our critical infrastructures and key assets present significant protection challenges. The entities involved are diverse, and the level of understanding of protection roles and responsibilities differs accordingly. Furthermore, these organizations and individuals represent systems, operations, and institutional cultures that are complex and diverse. The range of protective activities that each must undertake is vast and varies from one enterprise to the next. Finally, overlapping protection authorities across federal, state, and local jurisdictions vary greatly. Success in implementing a wide range of protection activities lies in establishing a unifying organizational framework that allows the development of complementary, collaborative relationships and efficiently aligns our protection resources.

Many jurisdictions are attempting to reinforce and expand anti-terrorism efforts by enhancing and integrating security planning and preparedness measures by identifying and training response staff and establishing and resourcing organizations in conformance with the National Incident Management System (NIMS)[3]. This system (NIMS) was established by the US Secretary of Homeland Security and provides for the development of Incident Management Response compliance criteria and implementation activities at federal, state and local levels. It also

provides guidance and outlines support to jurisdictions and incident management and responder organizations as they adopt the system.

Fully implemented NIMS will provide a consistent, flexible, and adjustable national framework within which government and private entities at all levels can work together to manage domestic incidents, regardless of their cause, size, location, or complexity. This flexibility applies across all phases of incident management: prevention, preparedness, response, recovery, and mitigation. The challenge, however, is to fully implement the system not only to include our operational and response staffs but to engage those on the planning and design side of the equation to insure efficient and seamless actions in response to an incident by properly designing the facility to address operational needs.

Communication

Agencies need to coordinate the regional transportation security planning efforts, project implementation, project financing and operations with all stakeholders within their jurisdictions. Agencies and owners need to focus on the business practices specific to each stakeholder, make the stakeholders aware of any deficiencies and/or vulnerabilities they may encounter, any training opportunities identified, and any other resources necessary to bolster Transportation Security, by making Security Awareness part of an entity's every day Business Practices.

All stakeholders must work to enhances Up, Down & Sideways communications. In matters pertaining to security, agencies and those supporting agencies should provide enhanced awareness of security vulnerabilities to their projects and the system in general, and insure that any security issues are addressed as early as possible in the Planning, Design and Construction of Transportation projects, as part of the normal project lifecycle. In accomplishing this, however, agencies and their agents face another major challenge which is to consider the economic needs to design, build, operate and maintain transportation infrastructure, in accomplishing security goals at low cost to avoid draw down on our available capital that could otherwise be used for other transportation enhancements.

Best Management Practices

A cornerstone to an agencies success in approaching security is to look for and use Best Management Practices of other public and private transportation entities for the Transportation sector to address security. Many Best Practices for use in the area of highways, bridges and tunnels can be found in the Blue Ribbon Panel report and the "Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection" discussed earlier.

These documents begin with a Self–Assessment of security provisions by the owning agency, and go on to Response, contingency, and continuity plans. They include a review of vulnerability of information technology systems to "cyber attacks", the Integration of "lessons learned", improvements in overall security for the area under scrutiny, and "target hardening" of key assets. They also suggest some design guidance for transportation facilities.

Technology

A significant amount of technology for use in securing the transportation system is being made available. Without a doubt the possible applications of available technologies for use in countering a variety of threats is mind-boggling. To this end, a major challenge is the development of protocols for technology evaluation to allow owners to determine the best applications of products for local needs. The development of integrated homeland security systems along with testing, demonstration and training of those systems also remains a challenge. The designation of centers to have potential technologies evaluated for use in solutions to transportation security challenges would surely enhance an owner's ability to match the best technology to each security need and should be a national priority to accomplish.

Design Guidance

A major question for many owners is what engineering guidance should be given and how to find out what knowledge was "available". Some owners immediate response was to utilize the best practices suggested in the "Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection" and the Blue Ribbon Panel's report to develop design guidance for use on its bridges. For example, in its Bridges and Structures Design Manual[4] NJDOT required a vulnerability analysis be done for each bridge project regardless of the project type.

The assessment is required for rehabilitation, reconstruction, replacement or new bridge projects. Considerations in the assessment are to include but not be limited to:

1. The location of the bridge structure or tunnel.
2. Traffic usage of the bridge structure or tunnel.
3. Prominence or historical significance.
4. Environmental impact.
5. Public Services.

Designers are instructed to use judgment and advice of NJDOT staff and others' knowledge of the project and region to assess the vulnerability of bridge structures or tunnels. Further, this assessment is to be documented and included in the project's Design Appraisal Statement, which becomes a part of the project record.
After completion of the assessment, designers are then directed to consider appropriate countermeasures within the project documents to provide for their security. Recommendations for use of countermeasures should be based on a prudent assessment of the specific vulnerability assessment of the bridge and with concurrence of the department. Some suggested countermeasures include:

1. Restrict parking under a bridge structure.
2. Installation of surveillance cameras
3. Restrict the placement of vegetation
4. Restrict access to ventilation machinery in tunnels.
5. Detail installation of emergency shut-off mechanisms.
6. Restrict access to key details
7. Restriction of access to movable bridge machinery and operator's housing.
8. Detail the lighting to ensure surveillance.
9. Detail all components so that no component is concealed from view.
10. Prohibit the use of non-redundant members.
11. Protect all main load carrying members from direct impact
12. Locate utilities as to minimize their potential use as weapons

The department's guidance was intentionally drafted to provide broad guidance to a designer realizing that new standards and practices were under development. This has provided a challenge, however, to designers to whom, like the Department, this requirement is very new. It requires designers to make new, bold recommendations, and this is causing a great deal of discomfort to them.

Cost

In their publication "Critical Issues in Transportation 2002,"[5] TRB made a statement that achieving security will be "difficult and costly but necessary." The general reaction is that achieving security is difficult and necessary, and that the need to find ways to make it cost-effective and part of the normal design. For the existing inventory, owners need to assess vulnerabilities, rank assets, then apply detection, deterrence, defense, reaction and recovery strategies to most efficiently respond to threats to our transportation system.NJDOT encourages consideration of the complete spectrum of strategies to find the best fit – detect, deter, deny, defend, response and recovery. The Department stresses to its designers default to hardening. Designers must incorporate an all hazards approach to design capitalizing on other detailing to address multiple hazards. Insuring that minimal if any, cost is incurred in designing for security so that in addressing security, agencies are not playing into terrorist's objectives of impacting our economy.

CONCLUSION

Our intent in writing this paper was to outline New Jersey's efforts in the area of transportation security, and to lists some of the opportunities and challenges still to come. As we have outlined, since 9/11 New Jersey has not hesitated to be proactive in addressing the security needs before us. In this paper we have outlined just a snapshot of the activities that have occurred to date and only briefly discussed several of the major challenges we are working on along with some of the opportunities we have encountered. Security is an elephant size challenge but we know how to eat an elephant – one bite at a time!

REFERENCES

1. "Recommendations for Bridge and Tunnel Security", Requested by: The American Association of State Highway and Transportation Officials Transportation Security Task Force, Prepared by: The Blue Ribbon Panel on Bridge and Tunnel Security, Published by U.S. Department of Transportation, Federal Highway Administration and the American Association of State Highway and Transportation Officials, September, 2003
2. "A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection", Prepared for The American Association of State Highway and Transportation Officials' Security Task Force, Prepared by Science Applications International Corporation (SAIC) Transportation Policy and Analysis Center National Cooperative Highway Research Program Project 20-07/Task 151B
3. "National Incident Management System", US Department of Homeland Security, Washington DC, March 1, 2004
4. "New Jersey Department Of Transportation Bridges and Structures Design Manual", Fourth Edition, 2002, NJDOT, Trenton, NJ
5. "Critical Issues in Transportation – 2002", *TR News* 217 November–December 2001, Transportation Research Board, The National Academies