The Inherent Challenges of Securing Transportation Infrastructure: Examination of the National Capital Region

Theodore A. Smith
Critical Infrastructure Protection Project
National Center for Technology and Law
George Mason University School of Law
3301 North Fairfax Drive, MS 1G7
Arlington, VA 22201
tsmithj@gmu.edu, theodore.smith@mitretek.org

ABSTRACT

Surface transportation systems are a critical element of virtually every aspect of life in the United States. They support national defense, move people and goods, employ millions of people, generate revenue and consume resources and services generated by other sectors of the economy. The terrorist attacks of September 11th had a significant impact on the United States, not only in terms of loss of life and property, negative economic impacts, but also with the unsettling realization that an inherently free society renders critical infrastructure in the United States susceptible to future attacks.

This paper examines the inherent challenges that transportation service providers and public safety agencies face in securing transportation infrastructure in the National Capital Region (NCR). In addition, this paper examines various planning, development, and operational activities that have been executed in the NCR to foster more secure transportation systems. This paper concentrates on highway networks, public transportation systems (including rail and buses), railways, and airport ground access networks.

Transportation infrastructure security is approached in this paper from the perspective that ensuring transportation infrastructures is not merely a process ensuring that an event such as a malevolent attack does not occur. Rather, the process also entails developing and implementing strategies and measures that specifically focus on responding to and recovering from the loss of an asset.

Key words: National Capital Region—security challenges—transportation security
BACKGROUND

Surface transportation systems are a critical element of virtually every aspect of life in the United States. They support national defense, move people and goods, employ millions of people, generate revenue, and consume resources and services generated by other sectors of the economy. In 2003, the transportation sector of the U.S. economy contributed $1.150 trillion to an $11 trillion gross domestic product (GDP) (BTS 2001). This is not surprising, considering that the United States is one of the most mobile nations in the world, accommodating over 3 trillion miles of passenger travel annually on highways and public transit systems (FHWA 2005). In 2003, there were also an estimated 196 million licensed drivers and over 134 million registered vehicles (private and commercial) in the United States (FHWA 2003). Further, public transit users made more than 9 billion unlinked trips using the more than 6,000 transit properties in 2003 (APTA 2005).

The terrorist attacks of September 11, 2001 had a significant impact on the United States, not only in terms of loss of life and property and negative economic impacts, but also with the unsettling realization that an inherently free society renders critical infrastructure in the United States susceptible to future attacks. Asa Hutchinson, Undersecretary for the Border and Transportation Security Department of Homeland Security (DHS), concludes that “whenever we are in a free society there will always be vulnerabilities that you can point to. That is an absolute rule of American Freedom” (Hutchinson 2003).

This paper examines the inherent challenges that transportation service providers and public safety agencies face in securing transportation infrastructure in the National Capital Region (NCR).1 In addition, this research examines various planning, development, and operational activities that have been executed in the NCR to foster more secure transportation systems. This paper concentrates on highway networks, public transportation systems (including rail and buses), railways, airport ground access networks, and postal and shipping systems. This paper is based on work conducted as part of the National Capital Region Critical Infrastructure Vulnerability Assessment Project, executed through the National Center for Technology and Law at the George Mason University School of Law, under grants from the Urban Area Security Initiative and the Department of Justice Community-Oriented Policing Program.

National Capital Region Transportation Systems

The NCR covers more than 3,000 square miles in the Commonwealth of Virginia, State of Maryland, and the District of Columbia and is currently home to some 4.2 million people and 2.7 million jobs. Supporting the movement of people and goods in the NCR is a vast transportation network that includes 14,100 lane miles of highways, more than 200 miles of carpool lanes, 103 miles of metrorail, and 162 additional miles of commuter rail. The system also includes an extensive bus network or local and commuter services, as well as three major airports: Ronald Reagan Washington National, Dulles International, and Baltimore/Washington International, and more than 10 general aviation airports (NCRTPB). Figure 1 illustrates the complex highway network in the NCR (from a Rand-McNally map).

---

1 The NCR is defined in the United States Code [40 USC 71 (b)] as the District of Columbia; Montgomery and Prince Georges Counties in Maryland; Arlington, Fairfax, Loudoun, and Prince William Counties in Virginia; and all cities existing in Maryland or Virginia within the geographic area designated by the outer boundaries of the combined counties listed. For consistency with the Metropolitan Washington Council of Governments (WashCOG) this research expands the definition of the NCR to include Frederick County in Maryland.
NCR Transportation Systems

The definition of the transportation systems that are a focus of this paper are in part based on Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001 and the National Infrastructure Protection Plan, The Physical Protection of Critical Infrastructures and Key Assets, February 2003. For the purposes of this paper, each mode within the transportation sector is composed of fixed infrastructure, such as facilities, roadways, information systems, and voice and data communications systems; vehicles and conveyance systems; and human capital at the state, local, and federal levels of government and civilian employees responsible for the development, operation, and management of transportation systems. Specific modes of transportation considered in this paper include the following:

- **Highway system.** This includes the physical facilities themselves, including roadways, bridges and tunnels, inter-modal terminals, maintenance facilities, vehicles (private and commercial motor carriers) operating on the system, and the control and information infrastructure that monitors and manages the flow of goods, vehicles, and people on the highway system (SAIC 2002; Physical Protection 2003).
- **Transit system.** This includes bus, rail, or other conveyance, either publicly or privately owned, that provide the public general or special service (but not including school buses or charter or sightseeing services) on a regular and continuing basis. System components include all of the vehicles, equipment, right-of-way, routes, support equipment and facilities, and buildings and real estate belonging to or operated by the public transportation authority (US DOT 2003).
- **Rail system.** Rail system infrastructure management elements include track maintenance throughout the NCR and the vehicles that operate on and adjacent to these facilities.
- **Airport ground access systems.** All of the vehicles, equipment, right-of-way, routes, support equipment and facilities, and buildings and real estate that provide ground access to Washington Reagan National Airport, Dulles International Airport, and Baltimore-Washington International
Airports. This paper does not address terminal and airfield operations and their related security challenges.

**Dimensions of Transportation Infrastructure Security**

Transportation infrastructures present three unique dimensions to the challenging task of securing transportation infrastructure. First, transportation infrastructure must be secured and protected from malevolent attacks that destroy, damage, or otherwise reduce the level of service provided by the given system as they, as mentioned, support national defense, move people and goods, employ millions of people, generate revenue, and consume resources and services generated by other sectors of the economy. It is also important to note that in order to ensure that transportation infrastructure is afforded the highest level of security possible other events, such as natural disasters and major incidents that are not man-made, must also be considered. Second, transportation systems themselves can be a vehicle or method of delivery for a malevolent attack. Although many examples can be sited to illustrate this, perhaps no event illustrates this challenge better than the terrorist attacks of September 11, 2001, when commercial airliners were used to carry out attacks. Third, the interdependencies among multiple infrastructure sectors necessitate that transportation security activities consider many things outside the transportation domain. As an example, the emergency service sector (police, fire, and emergency medical services) is dependent on the transportation sector to transport emergency resources and patients. Without a functioning transportation infrastructure, these functions may be impossible.

**FEMA Disaster Lifecycle**

Given the varying dimensions of transportation infrastructure security challenges, this paper is approached from the perspective that ensuring transportation infrastructures is not merely a process ensuring that an event such as a malevolent attack does not occur. Rather the process also entails developing and implementing strategies and measures that specifically focus on responding to and recovering from the loss of an asset. This is necessary, as it is understood that this collection of infrastructures are vulnerable and quite susceptible to failures due to their accessibility; the expansive and open natures of these infrastructures contribute to their vulnerability. Accordingly, to provide structure to the discussion and analysis, this paper presents issues in the context of what is commonly referred to as the Federal Emergency Management Administration (FEMA) disaster life-cycle. The FEMA disaster life-cycle is a series of activities that a region engages in to prepare for and respond to emergencies and disasters, help people and public and private institutions recover from emergencies and disasters and the effects of the emergency or disaster, reduce the risk of loss, and help prevent disasters and emergencies from occurring (FEMA 2003). Although variations of the disaster life-cycle have been used by others, for the purposes of this paper, the process includes the following:

- **Response.** This involves the mobilization and positioning of emergency equipment and personnel to get the public out of danger; bring the impacts of the disaster under control; provide basic necessities, including food, water, shelter, and medical services to those impacted by the disaster; and bring transportation systems and services back on line as soon as possible.
- **Recovery.** This involves repairing and/or replacing transportation infrastructure and vehicles in order to return them to their pre-disaster levels of service.
- **Risk reduction and prevention.** This involves reducing the probability of an attack on transportation infrastructure and mitigating the potential impacts should an attack occur.
- **Planning and preparedness.** This ensures that if a disaster occurs, transportation and public safety agencies, among others, are ready to respond in the safest and most efficient manner while ensuring the safety of the general public.
INHERENT CHALLENGES FROM A MODAL PERSPECTIVE

Highway

Quite possibly the most significant factors underlying the challenges associated with securing highway infrastructure, including bridges and tunnels, is that by design they are easily accessible to almost anyone and they transverse relatively long distances. Consequently, it is many times not feasible, or possible, to secure the entire highway network, whether through strategies such as surveillance, law enforcement patrols, or infrastructure hardening. Closely related to the inefficiencies of providing surveillance or monitoring of the entire highway network is the threat that commercial vehicles can possibly be targets of hijacking and consequently used as a means for carrying out malevolent attacks.

It is understood that, from an operational perspective, highway systems in the NCR are critical in moving people and goods, not only within the region, but also through it to other destinations nationally and internationally. Highway networks in the NCR are not necessarily susceptible to a single point of failure. For example, if a bridge crossing the Potomac River were to be lost, there are alternate means to move people and goods across the river. Loss of an asset such as a bridge crossing the Potomac River for any length of time, however, would have significant impacts on regional mobility. Loss of such an asset for an extended period of time would ultimately impact the economic vitality of the region. These impacts partially result from the fact that the NCR already suffers from some of the worst congestion in the United States, even when transportation systems are operating under normal conditions.
Also from an operational perspective, and closely related to the issue of limited capacity, are the challenges associated with evacuating the region in the event of an emergency using the existing highway system. As was demonstrated in the NCR following the terrorist attacks of September 11, 2001, rapidly moving masses of people out of the central city in a limited amount of time greatly compounds the mobility challenges of normal peak-hour flows. This challenge could be made exponentially worse if a highway asset such as a bridge or tunnel were lost during an attack. Ultimately, the inability to move people out of an urban core can compromise personal safety.

Planning for measures to prevent, respond to, and recover from transportation emergencies also presents a variety of challenges. Planning must be approached from the perspective that the systems work collectively to provide regional mobility. This can be especially challenging when multiple jurisdictions and service providers are involved. Consequently, the NCR provides an environment that too often exacerbates the inherent turf issues associated with regional planning activities. This is critical, in that if highway networks are to provide the safest and most efficient movement of people and goods, both during emergencies and during normal operations, the network must be planned and operated from a regional perspective.

Transit

History has also taught that transit facilities are attractive targets of malevolent attacks throughout the world. Between 1997 and 2000, more than 200 terrorist attacks were carried out worldwide on transit systems. These attacks involved, among other things, hijacked vehicles, chemical attacks, bombs, poison gas, guns, and grenades (Gersten and Jenkins 2001).

These threats are of particular concern because transit systems in the NCR provide similar opportunities for significant death and destruction, as they generate large volumes and densities of travelers with quite predictable patterns. In 2002, the Washington Metropolitan Transit Authority (WMATA) accommodated a combined total of 328.7 million bus and rail transit trips in the NCR. Factors that make the Metrorail specifically an attractive target of malevolent attacks include the following:

- There is relatively little redundancy in the system of tracks, which makes maneuvering trains difficult.
- A back-up operations center does not exist.
- Local transit service providers depend on WMATA to provide regional connectivity.
- To maintain operational efficiencies, it is impossible to screen passengers in a manner comparable to that of commercial air travel.

With respect to WMATA’s Metrorail system, biological or chemical agents could be spread to many, if not all, of the system’s 86 stations before being detected. Consequently, large portions of the system would be rendered unusable for long periods of time while cleanup activities are being conducted, dramatically extending recovery times. This could be catastrophic from a regional mobility perspective, since more than 40% of the work trips to the urban core of the NCR are made via public transit (WMATA).

Rail

The NCR has rail lines that pass directly through the center of the region. Consequently, there is significant concern with respect to the transportation of large amounts of hazardous materials. The primary concern is that significant numbers of injuries and loss of life could result should hazardous
materials be released as a result of an accident or malevolent attack. A loss of a bridge or a tunnel that supports rail operations could also have long-term adverse impacts on the economy, through, among other things, disruptions in supply chains and infrastructure repair and replacement costs.

With this issue in mind, on February 1, 2005 the District of Columbia City Council approved emergency legislation restricting the shipment of hazardous materials within two miles of the U.S. Capitol and federal buildings. The legislation requires rail and trucking companies to receive a special permit before they can transport large quantities of hazardous chemicals through the District of Columbia. C-S-X is suing the city and asking a federal judge to strike down its ban on hazardous train shipments. Although the issue has yet to be resolved, it has the potential to impact the transportation of hazardous materials in other regions. Of particular concern with respect to this issue are the potential impacts that such restrictions could have on interstate trade.

Airport

Ground access to Dulles International Airport and Ronald Reagan Washington National Airport has been significantly impacted since the attacks of September 11th. Measures implemented to enhance security, such as prohibiting motorists to park on the terminal drives, has impacted the flow of traffic. Both airports have been forced to implement strategies, such as barrier walls, that have also disturbed the operation of the airport approaches. Accordingly, the challenges presented by peak traffic volumes are exacerbated when the given measure is put in place. Furthermore, given the unrestricted access to the airports, very little can be done to prevent a malevolent attack on a terminal, parking structure, or roadway network under current operating conditions, regardless of measures that have been put in place.

OTHER TRANSPORTATION SECURITY CONSIDERATIONS

Transportation Stakeholders and Interdependencies

The diverse and complex composition of transportation stakeholders in the NCR in itself presents a variety of challenges that can affect transportation security. The inherent multi-modal nature of the services provided and the sizable number of jurisdictions in the NCR creates an environment that necessitates a large number of stakeholders who are all in some way responsible for the planning, development, operations, management, and security of the various systems. Bringing multiple stakeholders together to achieve a common goal can be challenging, especially when transportation agencies and service providers must consider the needs and interests of the entire region first, and their individual needs and interests second. Adding to the complexity is that operating agencies at the federal, state, and local levels, as well as in the private sector, all play integral roles in the delivery of services.

As mentioned, it also important to understand the interdependencies of other infrastructure sectors. Figure 3 illustrates some of the dependencies that other sectors have on the transportation sector, and vice-versa. As an example of interdependencies, the safe and efficient operation of some transportation systems (highway and transit) is not possible without the services of other critical infrastructures. As an example, if traffic signals are not equipped with uninterruptible powers supplies (UPS), traffic signals are rendered inoperable when power to the signals is lost. Loss of power can also render some or all rail operations inoperable. Each of these sectoral dependencies, among others, illustrated in Figure 3 are underpinned by a complex set of institutional and operational arrangements that have been developed to maximize the efficiency and reliability of each of the sectors.
Lack of Voice Communications

Generally, from an operational perspective, at the local level there is also a chronic lack of voice and data communications systems interoperability among responding agencies from various disciplines and jurisdictions. A study sponsored by the National Institute of Justice, National Task Force on Interoperability concluded that a variety of factors are impediments to interoperability of voice and data communications systems, including the following:

- Communications equipment is aging and incompatible. Adjacent jurisdictions often use different types of radio systems and different frequencies.
- Funding is limited and fragmented. Resources for replacement of voice and data communications systems are limited at every level of government.
- Planning is limited and fragmented. Planning activities are typically underfunded and are rarely conducted in the context of the region as a whole.
- There is a lack of coordination and cooperation. Agencies are often reluctant, if not unwilling, to give up management and control of their own voice and data communications systems at any level of planning, development, implementation, or operation.

Additionally, attacks on transportation infrastructure involving weapons of mass destruction pose even more complicated response challenges. Responding to such attacks requires a combination of trained personnel, specialized equipment, well-defined procedures, and supplies. The challenge lies not only in having access to these resources, but having access to a sufficient number of these resources. For
example, an attack on a WMATA Metrorail that could literally affect thousands of people at one time would likely be overwhelming for all of the involved response agencies.

OVERCOMING THE CHALLENGES IN THE NATIONAL CAPITAL REGION

The inherent challenges of securing transportation infrastructure facing federal, state, and local agencies are unlike any that the United States has ever faced. The threats have no boundaries, either jurisdictionally or in terms of disciplines they affect. To secure transportation infrastructure adequately, stakeholders in the NCR have begun to embrace new measures to enhance security. Described below are descriptions of such initiatives that have been executed in the NCR.

Department of Homeland Security, Office of National Capitol Region Coordination

Recognizing that the federal government was not organized, staffed, nor adequately prepared to meet the changing demands of the 21st century (including preventing terrorist attacks and securing transportation infrastructure), President George W. Bush proposed draft legislation to Congress to create the Department of Homeland Security (DHS) on June 18, 2002. The passage of the legislation and the subsequent creation of the DHS represented the largest reorganization of the federal government since the outbreak of the Cold War, when the National Security Act of 1947 unified the Armed Forces under a single department and created the National Security Council and the Central Intelligence Agency.

With respect to influence on the NCR, the Office of National Capitol Region Coordination (ONCRC), located within the DHS, has been charged with overseeing and coordinating federal programs and domestic preparedness initiatives for state, local, and regional authorities in the NCR. ONCRC has been an instrumental player in the many initiatives that have been carried out in the NCR by the Metropolitan Washington Council of Governments (WashCOG) and its member agencies, including the development of the Regional Emergency Coordination Plan and its ancillary components that are described below.

Regional Emergency Coordination Plan

Initial evaluations of WashCOG’s security planning following the attacks of September 11th indicated that the components of the regional transportation system performed fairly well individually (Wegmann). Collectively, however, at the regional level coordinating among the various transportation service providers fell short. Consequently, the Transportation Planning Board (TPB) was charged with developing a coordinated emergency response plan.

In response to this challenge, the TPB developed the Regional Emergency Coordination Plan (RECP) to provide a vehicle for collaborating in planning, communication, information sharing, and coordination activities before, during, or after a regional emergency for the 17 WashCOG member governments, the State of Maryland, the Commonwealth of Virginia, the federal government, public agencies, private sector and volunteer organizations, and local schools and universities.

Regional Integrated Communication and Coordination

The Regional Integrated Communication and Coordination Systems (RICCS) provides a system for WashCOG members, the State of Maryland, the Commonwealth of Virginia, the federal government, public agencies, private sector and volunteer organizations, and schools and universities to collaborate in planning, communication, information sharing, and coordination activities before, during, and after a
regional incident or regional emergency. RICCS utilizes a variety of new and existing communication devices to foster collaboration that will be critical in the event of an emergency that has regional impacts.

**Regional Emergency Evacuation Transportation Coordination**

The Regional Emergency Evacuation Transportation Coordination (REETC) is intended to address the transportation aspects of moving people around or out of the region and moving required resources into the area in anticipation of and following a regional incident or emergency that requires evacuation. Therefore, REETC addresses coordination of demand management, identifying situations and strategies where the majority of people do not evacuate the area, but shelter in place to ensure that transportation system capacity is available for those who truly need it.

**Capital Wireless Integrated Network**

The Capital Wireless Integrated Network (CapWIN) project is a partnership between transportation and public safety agencies in the State of Maryland, the Commonwealth of Virginia, and the District of Columbia. The focus of this initiative is to develop an integrated transportation and criminal justice information wireless network. CapWIN will integrate transportation and public safety data and voice communication systems in the two states and the District of Columbia and will be the first regional transportation and integrated wireless network for public safety in the United States. CapWIN will enable critical and time-sensitive data to reach responders in other jurisdictions throughout the region.

**CapCOM**

In late 2004 TPB requested $5 million from the United States Congress to develop CapCOM, which may best be characterized as an operations center that will be implemented to foster regional operations coordination for surface transportation systems. This new initiative is envisioned to function similarly to TransCom in the New York/New Jersey/Connecticut tri-state area and provide a governance structure for regional transportation operations during normal and emergency operations. TransCom was widely regarded as essential in evacuating Manhattan during the attacks on the World Trade Center.

The primary motivations for initiating this effort stem from the absence of one single entity that is in charge of coordinating regional operations in real-time and managing incidents that have a regional impact. Managing such incidents has become a priority for transportation and public safety agencies in the region. The two primary functions of CapCom will be regional operations support and regional planning and preparedness. CapCOM development efforts in 2005 have focused so far on developing the supporting governance structures.

**PRELIMINARY FINDINGS**

Transportation systems in the NCR are critical in supporting the movement of people and goods. A loss of any number of transportation assets or a prolonged reduction in the level of service provided by the systems would likely result in serious economic impacts to the region. Consequently, it is critical that transportation systems are provided with the highest level of security possible to protect them from natural disasters, major incidents, and malevolent attacks.

To secure transportation infrastructure in the NCR, it will be necessary for the regional partners to overcome the inherent challenges associated with this phase of the process. Furthermore, it is becoming increasingly important to continue the shift of planning, operations and management, and systems
procurement activities from a system that has a localized focus to one that considers such activities in the context of the entire region. The NCR has made significant progress with respect to this challenge as demonstrated in the development of the Regional Emergency Coordination Plan, the Regional Information Communication and Coordination Systems, CapWIN, and CapCOM.
REFERENCES


