A Framework for Planning Cost-Effective Rail Security Against a Terrorist Attack

This product is part of the RAND Corporation research brief series. RAND research briefs present policy-oriented summaries of published, peer-reviewed documents.

www.rand.org

Each weekday, more than 12 million passengers take to U.S. railways. While there have been no successful attacks on U.S. rail systems recently, attacks on passenger-rail systems around the world—such as the London Underground in 2005—highlight the vulnerability of rail travel and the importance of rail security for passengers.

RAND researchers have developed a framework for security planners and policymakers to guide cost-effective rail-security planning, specifically for the risk of terrorism, and demonstrated its use on a notional intracity rail system that characterizes rail systems typically found in the United States.

From Where Is the Threat Likely to Come?
Drawing primarily on available data on past terrorist attacks on rail systems from the RAND-MIPT Terrorist Incident Database, the study found that bombings are the most prevalent terrorist threat to rail systems; that most such attacks produce few fatalities and injuries; and that attacks in densely packed rail cars and interior rail-facility locations are of particular concern because of the casualties they can produce. Not all such attacks come from explosives, so security measures must address both explosive devices and the possibility of rarer attack modes. Also, given the damage from a relatively small number of large attacks, security measures that prevent only the largest-scale attacks could significantly reduce the associated human costs.

How and Where Is a Rail System Most at Risk?
To understand how to protect rail systems, we examined 11 potential attack locations in a rail system and then subjected them to eight potential attack modes. Each of the resulting scenarios was then categorized as high, medium, low, or no risk. (The latter occurs when the target-attack

Abstract

U.S. communities depend on reliable, safe, and secure rail systems, but such systems are vulnerable to terrorist attack. This brief explains a framework for security planners and policymakers to guide cost-effective rail-security planning and applies it to a notional rail system that characterizes rail systems typically found in the United States. While the analysis results are specific to the notional system, the framework itself is useful for planning rail-security options.

combination is not possible.) The figure shows the results of that qualitative filtering.

We note that some rail-attack modes are more of a concern than others. For example, the use of small explosives is a high or medium risk for most targets, while hoaxes or threats pose a risk for only a few targets. Second, some targets are more of a concern than others. For example, the target of system-operation and power infrastructure is a high or medium risk for seven of the eight attack modes. Then again, underground infrastructure is less of a target when assessed against the attack modes.
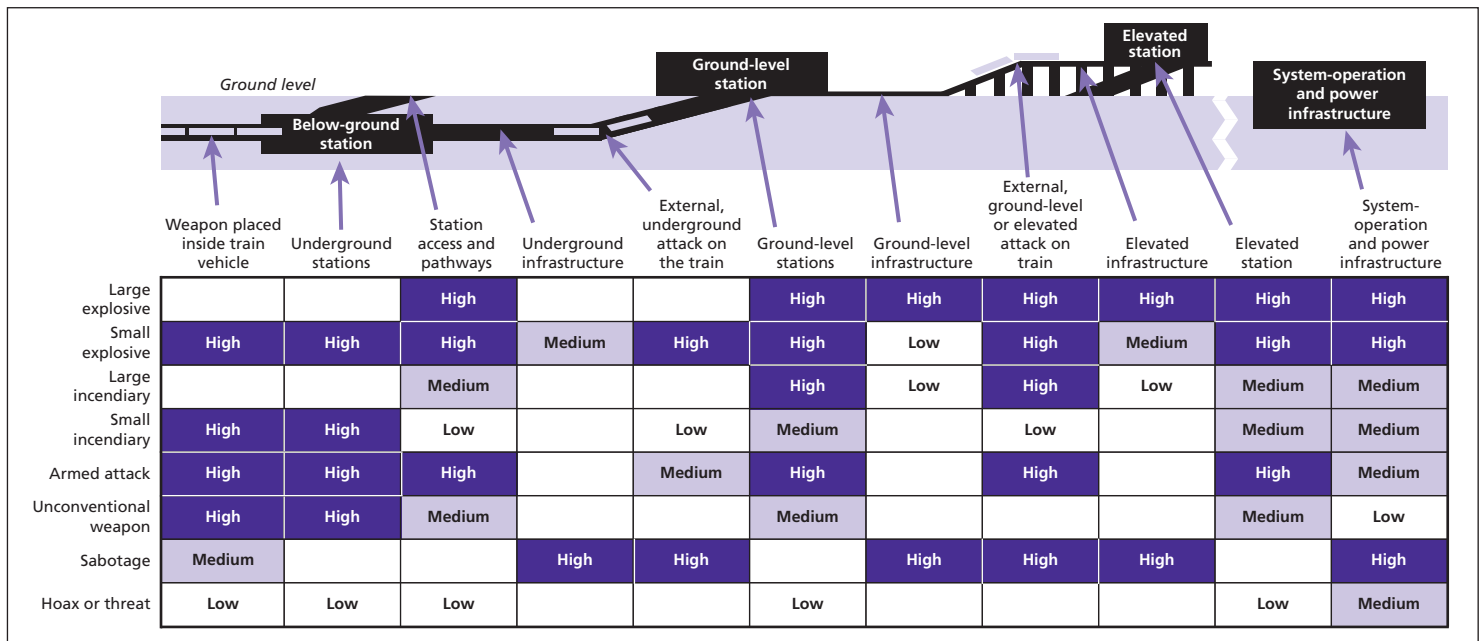
How Can We Think About Protecting a Notional Rail System?
In thinking about how to defend rail systems, we started with a relatively simple, notional rail network located within a major metropolitan area, consisting of five spokes of unique rail lines going directly into one hub station, with the only transfer point between these lines located at the hub station. We assumed that the notional rail-security system would have some security measures in place. Finally, we adopted a Federal Transit Administration vision of a multilayered

	Weapon placed inside train vehicle	Underground stations	Station access and pathways	Underground infrastructure	External, underground attack on the train	Ground-level stations	Ground-level infrastructure	External, ground-level or elevated attack on train	Elevated infrastructure	Elevated station	System-operation and power infrastructure
Large explosive			High			High	High	High	High	High	High
Small explosive	High	High	High	Medium	High	High	Low	High	Medium	High	High
Large incendiary			Medium			High	Low	High	Low	Medium	Medium
Small incendiary	High	High	Low		Low	Medium		Low		Medium	Medium
Armed attack	High	High	High		Medium	High		High		High	Medium
Unconventional weapon	High	High	Medium			Medium				Medium	Low
Sabotage	Medium			High	High		High	High	High		High
Hoax or threat	Low	Low	Low			Low				Low	Medium

transportation-security system, in which we defined security layers going from safeguarding the outermost perimeter to the exterior, interior, and restricted-access areas to the innermost rail-security asset, the trains.

Having defined the notional system's existing security, we identified 17 security-improvement options and assessed their relative effectiveness across the security layers. We evaluated effectiveness by assessing how well the options prevented or reduced the probability of a specific terrorist attack occurring, reduced or averted the number of passenger fatalities in the system, reduced the time necessary for system facilities and infrastructure to be restored and operations fully resumed, and minimized rail-operating revenue losses. We rated options in terms of both their incremental impact at each layer and their potential system-level contribution across layers.
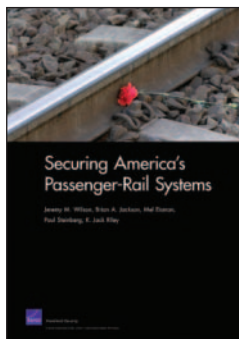
At the system level (integrating across layers), we identified four broad categories of cost-effective security measures for system operators to consider in terms of effectiveness for dollar metric payoffs: (1) relatively inexpensive solutions with the highest effectiveness (e.g., enhanced security training); (2) additional inexpensive solutions to consider with reasonable levels of effectiveness (e.g., installing retractable bollards at entrances and exits of the operation-control center and power plant); (3) costlier solutions with highest effectiveness (e.g., installing fixed barriers at curbsides adjacent to all entrances and passageways leading to ground-level and underground stations); and (4) relatively expensive, longer-term solutions for future consideration (e.g., rail-vehicle surveillance systems).

Conclusions

The prioritized options are specific to the notional system analyzed, and the analysis captures a point in time, such that the current costs for those options and their current perceived effectiveness drive the attractiveness of different options. Thus, even if the preferred options are viewed as reasonable for a given system, even that conclusion is perishable.

These limitations notwithstanding, the framework itself is useful for planning rail-security options but should be tested against other systems of varying complexity. Such testing will yield two insights. First, it will help us better understand whether the portfolio of preferred options varies with system complexity or is largely the same regardless. Since risk and the nature of preexisting measures vary by the type of system examined, such testing will also give some insight into the dynamic nature of the threat and security assessment process and, perhaps, the timeline over which the assessments need to be repeated to counter the fact that terrorists wield new methods and learn their potential targets' defenses over time. Second, applying the framework to systems of differing complexity will allow us to better understand the information demands that the framework imposes. ∎

Homeland Security

A RAND INFRASTRUCTURE, SAFETY, AND ENVIRONMENT PROGRAM

This PDF document was made available from www.rand.org as a public service of the RAND Corporation.

This product is part of the RAND Corporation research brief series. RAND research briefs present policy-oriented summaries of individual published, peer-reviewed documents or of a body of published work.

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world.

Support RAND

Browse Books & Publications

Make a charitable contribution

For More Information

Visit RAND at www.rand.org

Explore the RAND Homeland Security Program

View document details