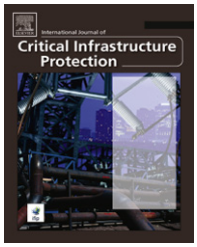
available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/ijcip



Security and the US rail infrastructure☆

Mark Hartong[a,*], *Rajni Goel*[b,1], *Duminda Wijesekera*[c,2]

[a] *Federal Railroad Administration, 1200 New Jersey Ave SE, Washington, DC 20590, United States*
[b] *Howard University, Information Systems and Decision Sciences, School of Business, 2600 6th Street, Washington, DC, United States*
[c] *George Mason University, Department of Computer Science, MS 4A4, 100 University Drive, Fairfax, VA 22030, United States*

ARTICLE INFO

Article history:
Received 4 July 2008
Received in revised form
19 August 2008
Accepted 20 August 2008

Keywords:
Railroad
Security
Vulnerabilities

ABSTRACT

Railroads play a significant role in the United States economy, transporting a wide variety of goods across a geographical disperse network. Hardening this network against all forms of attack is not possible. This paper will address the role of freight and passenger rail in the United States, provide an unclassified set of relatively easy attacks that can be used to disrupt rail traffic, outline actions by industry and government to reduce the probability of an attack occurring or mitigate the consequences of a successful attack, and identify shortcomings in the current rail security program.

Published by Elsevier B.V.

1. Introduction

Railroads are a critical transportation asset and play a significant role in the United States economy transporting a diverse mixture of commodities (Fig. 1) that supports all facets of the US industrial base. They operate in every state in the US except Hawaii, across a network (Fig. 2) that exceeds 140,000 miles [1]. The scale of operations is massive. In 2006 the seven major Class 1 railroads alone employed over 167,000 people at an average total compensation of over $94,000 per individual, moving over 1.7 trillion ton miles of freight, with revenues exceeding $52 billion [2]. This equates to 25% of all intercity freight tonnage carried in the US, and 41% of all ton-miles, approximately 12% of all freight revenue in the US in ton-miles. Railroads also operate the 30,000 miles of the Department of Defense Strategic Rail Corridor Network (STRACNET) for the movement of Department of Defense munitions and other materials [3].

The hauled freight includes 1.7–1.8 million carloads of hazardous material [4], including one extremely hazardous subset known as Toxic by Inhalation (TIH) material. TIH materials are "gases or liquids that are known or presumed on the basis of test to be so toxic to humans as to pose a health hazard in the event of a release during transportation" [5]. Although TIH materials constitute only 0.3% of all hazardous material shipments by rail [6], this still equates to over of 21.6 million ton miles of TIH movements per year [7]. Railroads, hence, are a crucial yet sensitive component of the US transportation network.

Disruptions in railroad services can have a significant adverse impact on the US economy as well as military

☆ The views and opinions expressed herein are that of the author and do not necessarily state or reflect those of the United States Government, the Department of Transportation, or the Federal Railroad Administration, and shall not be used for advertising or product endorsement.

* *Corresponding address:* 4039 Lake Glen Dr, 22033 Fairfax, VA, United States. Tel.: +1 202 493 1332; fax: +1 202 493 6309.
E-mail addresses: mark.hartong@dot.gov (M. Hartong), rgoel@howard.edu (R. Goel), dwijesek@gmu.edu (D. Wijesekera).
[1] Tel.: +1 202 806 1649; fax: +1 202 797 6393.
[2] Tel.: +1 703 993 1578; fax: +1 703 993 1638.

1874-5482/$ - see front matter. Published by Elsevier B.V.
doi:10.1016/j.ijcip.2008.08.006

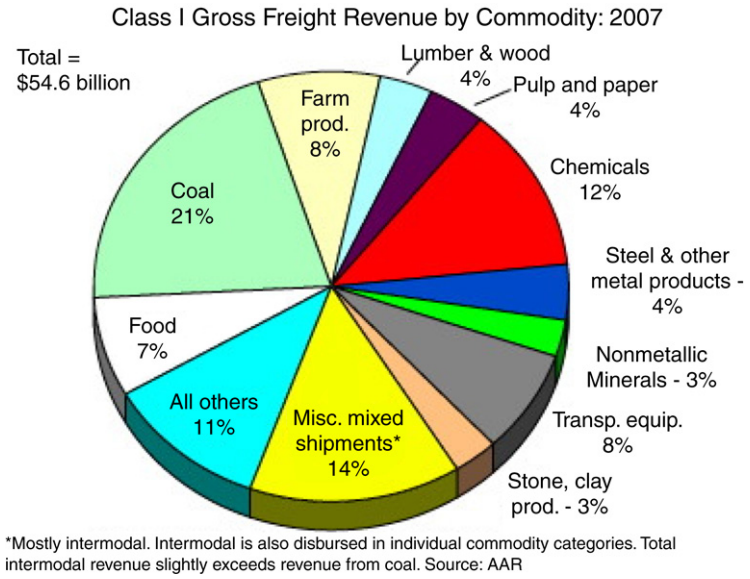


Fig. 1 – Class 1 commodity shipments (source AAR).

Fig. 2 – US rail network (source USCGS).

Fig. 3 – Graniteville, SC rail accident (source NTSB).

preparedness. The geographic dispersion of the railroad infrastructure, the manner in which it is constructed, and the ease with which an adversary can disrupt or damage it, precludes providing absolute security. Although the rail industry and the government have undertaken extensive efforts to protect the movement of freight and passengers, rail security remains an exercise in risk mitigation, as opposed to risk prevention. A determined adversary can exploit any one of a number of vulnerabilities, with potentially catastrophic consequences. These vulnerabilities are associated with both the physical and communication components of the infrastructure. While there are some additional steps that can be taken to reduce exploitable vulnerabilities, the fact remains that the system, and the public that it serves, will always be exposed to a measurable level of risk.

The consequences of the January 6, 2005 collision and derailment in Graniteville South Carolina [8] are representative of the potential losses resulting from a loss of tank integrity. In this particular accident (Fig. 3) the accidental release of chlorine gas from one ruptured tank killed 9 people, injured 554 people, required the evacuation of 5400 people with direct and indirect damages exceeding $40 million. A similar accidental release, in this case anhydrous ammonia, as the result of a derailment and tank car rupture in Minot, North Dakota killed 1 person, injured 333, and required the evacuation of 11,600 people [9].

This paper focuses on the potential vulnerabilities of the United States Rail Infrastructure, as well as possible mitigation strategies towards attacks. Section 2 provides a fresh background on the rail system, Section 3 details the vulnerabilities in the rail infrastructure, and Sections 4 and 5 discuss the mitigation strategies with some recommendations.