TRANSPORTATION SECURITY ADMINISTRATION
OFFICE OF INTELLIGENCE

(U) Freight Rail
Threat Assessment

28 February 2011

(U) Executive Summary

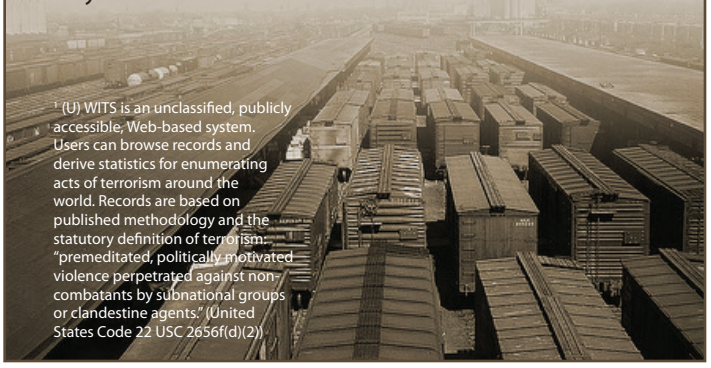
(U) Scope

(U//FOUO) The Transportation Security Administration's Office of Intelligence (TSA-OI) unclassified annual Freight Rail Threat Assessment addresses the overall threat to the U.S. freight rail industry and presents conclusions regarding likely targets and actors based upon a review of successful attacks against rail systems overseas.

(U//FOUO) The U.S. freight railroad sector incorporates 565 railroads operating on 139,679 miles of track throughout North America, including the United States, Canada, and Mexico. According to the Association of American Railroads (AAR), seven large freight, or Class I, railroad companies own and operate the majority of railroad track and rail property in the country. The AAR defines Class I railroads in the United States as those with the highest revenue. These seven Class I companies share trackage rights among themselves with shortline freight, and with commuter and passenger railroads. Freight railroads employ 168,891 people, maintain more than 1.5 million rail cars in North America, and transport approximately 43 percent of U.S. domestic freight and valuable commodities—including petroleum, chemicals, farm products, automobiles, food, lumber, and coal. Freight and passenger rail operations are often interdependent and use the same infrastructure, including track, signals, and in some cases control centers.

(U) Source Summary Statement

(U//FOUO) Much of the information presented below has been derived from information found in the National Counterterrorism Center's Worldwide Incidents Tracking System (WITS). TSA-OI reviewed rail-related attacks in WITS between 1 April 2009 and 31 March 2010. Other information found in this assessment is derived from intelligence and open source reporting. No single source dominated or had a particularly catalyzing effect on the analysis.



[1] (U) WITS is an unclassified, publicly accessible, Web-based system. Users can browse records and derive statistics for enumerating acts of terrorism around the world. Records are based on published methodology and the statutory definition of terrorism: "premeditated, politically motivated violence perpetrated against non-combatants by subnational groups or clandestine agents." (United States Code 22 USC 2656f(d)(2))

(U) Executive Summary (cont'd)

(U//FOUO) TSA-OI has no specific, credible intelligence to suggest violent transnational or domestic extremist groups are planning to attack the U.S. freight rail system, or use the system to facilitate an attack against another target. TSA-OI assesses with moderate confidence[i] that the risk of an attack to the U.S. freight rail industry is low.

- (U//FOUO) TSA-OI assesses with high confidence that passenger trains or stations are more likely to be targeted than freight trains. The interdependency of the freight and passenger rail infrastructure in the United States increases the likelihood that any threats or attacks against passenger rail could impact freight rail as well.

- (U//FOUO) TSA-OI judges that al-Qa'ida (AQ), its affiliates, and other terrorists motivated by violent extremist views would be the most likely actors to target the U.S. freight rail system. This judgment is based on recent attacks against freight rail and passenger trains overseas and the recent stated goals of al-Qa'ida's senior leadership to attack U.S. transportation.

- (U//FOUO) Based upon a review of worldwide attacks on freight rail targets, TSA-OI assesses that improvised explosive devices (IEDs) would be the most likely means of attack against the U.S. freight rail system.

- (U//FOUO) There is little evidence of a specific terrorist threat to freight rail Supervisory Control and Data Acquisition (SCADA) or other Industrial Control Systems (ICS), but al-Qa'ida and other violent extremist groups have a sustained interest in acquiring the skills to conduct cyber attacks.

i TSA-OI uses a three-point scale in which "High Confidence" generally indicates TSA-OI judgments are based on high-quality information and/or the nature of the issue makes it possible to render a solid judgment. "Moderate Confidence" generally means the information is interpreted in various ways, TSA-OI has alternative views, or the information is credible and plausible but not corroborated sufficiently to warrant a higher level of confidence. A "Low Confidence" judgment generally means the information is scant, questionable, or very fragmented and it is difficult to make solid analytical inferences, or TSA-OI has significant concerns or problems with the sources.

TSA-OI Freight Rail Modal Threat Assessment

(U//FOUO) TSA-OI assesses the terrorism threat to the U.S. freight rail industry is low. There has never been a confirmed attack on freight rail in the Homeland by a terrorist group, and the Intelligence Community lacks current or specific intelligence that terrorists intend to target domestic freight rail. Terrorist success in attacking rail systems overseas could inspire them to use similar tactics, techniques, and procedures against freight rail in the United States.

(U) Actors

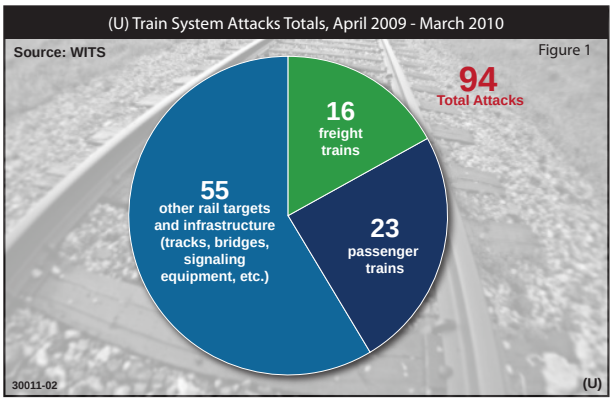
(U//FOUO) Although no terrorist organization has displayed an interest in attacking U.S. freight rail, TSA-OI judges AQ or affiliates would be most likely to do so because they have stated their intent to attack transportation modes and have successfully targeted rail in the past overseas.

(U//FOUO) Past intelligence reporting indicates terrorist groups have sought to use individuals with insider knowledge of transportation sectors to help facilitate an attack against the United States. Industry insiders in the freight rail business can include former and current railroad employees with extensive information about the railroad industry and railroad operations. TSA-OI is not aware of any known instance of insiders in the freight rail industry assisting terrorists to commit acts of terrorism; however, in September 2007, Adem Yilmaz, reportedly a member of the Islamic Jihad Union cell targeting Germany, was arrested while employed at the railway station of Frankfurt Airport. Yilmaz was employed in the security division of rail operator Deutsche Bahn from 1997 until 2002. During that time, Frankfurt Airport was one of several targets that his cell considered as a potential target.[1] TSA-OI has no information that proves Yilmaz used insider knowledge to target the airport. This group also discussed targeting other airports in Germany of which Yilmaz had no knowledge.

(U) Targets

(U//FOUO) A review of WITS data from April 2009 through March 2010 reveals 94 attacks on rail targets worldwide. Of those 94 attacks, only 16 appeared to specifically target freight trains; 23 attacks were made against passenger trains; and the remaining 55 attacks were committed against other rail targets and infrastructure—e.g., tracks, bridges, signaling equipment—that could have affected either freight or passenger rail. The targets and motivation for these attacks remain unknown.[2]

(U//FOUO) Recent statements from al-Qa'ida's senior leadership regarding striking U.S. interests including transportation could inspire attacks against rail targets in the Homeland.[3] Although al-Qa'ida likely considers passenger trains a higher priority target than freight trains, the interdependency of the freight and passenger rail infrastructure in the United States—bridges, tunnels, dispatch and control centers, tracks, signals and switches—increases the likelihood that threats or attacks against passenger rail could impact freight rail as well.



(U) Toxic Inhalation Hazards (TIH)

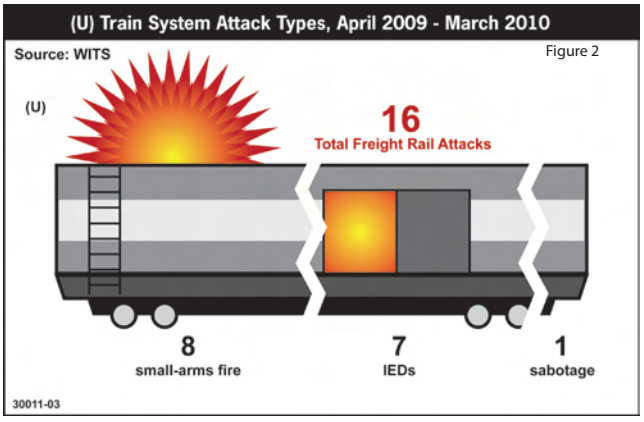
(U//FOUO) According to the Association of American Railroads Bureau of Explosives, each year, more than 76,000 bulk rail shipments of materials poisonous by inhalation, commonly referred to as toxic inhalation hazard (TIH), traverse nearly all major American cities and metropolitan regions. Because of its pervasiveness (more than 30,000 shipments per year) and toxic effects (500 parts-per-million can cause health problems), chlorine is of particular concern to the freight rail industry.

(U//FOUO) No terrorist group has ever attacked a rail car transporting TIH commodities. Additionally, TSA-OI has no current intelligence to indicate that al-Qa'ida or any other terrorist organization is planning to conduct an attack on a TIH car. Nevertheless, a successful attack on a freight rail car transporting TIH through a densely populated urban area could meet al-Qa'ida's strategic goals of attacking targets that would generate mass casualties, economic damage, and fear.[4]

(U) Tactics

(U) Improvised Explosive Devices (IEDs)

(U//FOUO) Worldwide, IEDs were the most common weapon used for attacking all components of the rail system (passenger and freight). IEDs were used in 71 of 94 attacks, or 76 percent, of attacks on all rail targets, including tracks, bridges, and other components of railroad infrastructure. Of the 16 attacks on freight rail, seven were conducted with IEDs, eight with small-arms fire, and one was determined to be an act of sabotage. As a result of the success of IED attacks against all railroads overseas,[5] TSA-OI assesses that terrorists would use IEDs in similar attacks on freight rail in the Homeland.



- (U) March 2010: Terrorists in the Republic of Dagestan in Russia blew up a freight train using a homemade, pressure-activated device containing approximately 2 kilograms of trinitrotoluene (TNT) that detonated as the train passed. The explosion set fire to the locomotive, derailed it and 14 empty cars, and damaged 250 meters of track. There were no casualties.[6]

- (U) February 2010: An IED detonated between two trains near a city rail station in southern Russia. One of the trains was carrying 28 tanks of aviation fuel.[7]

- (U) November 2009: Sixteen fuel-laden tanker cars were destroyed when suspected insurgents triggered an IED in Assam, India. Three hundred meters of track were also destroyed. The blast, resulting fire, and the damaged track disrupted the movement of trains throughout the region.[8]

(U) Assam Train Attack

(U) Vehicle-Borne Improvised Explosive Devices (VBIEDs)

(U//FOUO) Although terrorists worldwide have substantial experience in using vehicle-borne VBIEDs, TSA-OI has no evidence of a VBIED ever being used against either a freight or passenger train.[9]

(U) Cyber Attacks

(U//FOUO) Although there is little evidence of a specific terrorist threat to freight rail Supervisory Control and Data Acquisition (SCADA) or other Industrial Control Systems (ICS), intelligence reporting indicates al-Qa'ida and other violent extremist groups have a sustained interest in acquiring the skills to conduct cyber attacks.[10] Independent hackers, as well as foreign governments, have also been linked to repeated intrusions into U.S. business and control system computer networks.[11]

- (U//FOUO) In 2003, a U.S. freight rail company's business systems became infected with a non-directed computer worm. Much of the consequent degradation of rail operations stemmed from mitigation efforts to contain the intrusion, highlighting how computer system performance can be directly affected in unexpected or unanticipated ways (whether intentionally or otherwise).[12]

(U) Suspicious Incidents

(U//FOUO) While numerous suspicious incidents connected to the U.S. freight and passenger rail systems have been reported each year in the United States, none has been linked to terrorism. Most involved vandalism or tampering with rail tracks, and it was unclear whether freight or passenger rail was the actual target. Two of the more serious incidents follow:

- (U//FOUO) May 2009: A near collision occurred in Minot, North Dakota, when a train came upon two empty locomotives that had been moved and left standing on the single main line. The train crew initiated an emergency brake application and managed not to hit the locomotives. Local law enforcement reported that two youths were observed jumping off and running away from the two locomotives. The two locomotives were identified as switch engines that had been parked and left unmanned on a nearby siding.[13]

- (U//FOUO) March 2009: Track switches were surreptitiously reversed in separate incidents near Tewksbury, Massachusetts, and Nashua, New Hampshire, changing the direction of rail traffic. Additionally, at both locations, the perpetrator(s) replaced the railroad locks on the track switches with locks for which the railroad personnel lacked keys. The perpetrators may have been attempting to cause a collision or derailment of trains.[14]

(U) Outlook

(U//FOUO) TSA-OI has no specific intelligence indicating a credible or imminent threat to the U.S. freight rail system and assesses that the overall threat to the freight rail industry from terrorism is low. TSA-OI concludes, however, that terrorists would most likely use IEDs if they conducted attacks on rail in the Homeland. TSA-OI assesses that reporting and resolving suspicious activity is critical in aiding law enforcement and security officials with identifying unusual behavior, trends, patterns, and criminal acts that could precede terrorist operations.

(U//FOUO) Prepared by the TSA Office of Intelligence, Transportation Analysis Branch. For dissemination questions, contact TSA-OI_Production@tsa.dhs.gov.

Tracked by: HSEC-02-03003-ST-2009 Rail

(U) Endnotes

1 (U) Spiegel Online; 17 September 2007; "(U) Terror Suspect Worked at Frankfurt Airport;" (U)
2 (U) Worldwide Incidents Tracking System; http://wits.nctc.gov; 31 March 2010; (U)
3 (U) DHS IA-0291-10, "(U) Evolution of the Terrorist Threat to the United States," 21 May 2010; (U//FOUO)
4 (U) CIA; CTC 2003-30053; 7 July 2005; (U//FOUO)
5 (U) Worldwide Incidents Tracking System; http://wits.nctc.gov; 31 March 2010; (U)
6 (U) OSC; CEP20100315004003; 11 MAR 10; "(U) RUSSIA: Militants Carry Out Further 'Acts of Sabotage' In Dagestan, Ingushetia;" (U)
7 (U) OSC; CEP20100315004003; 11 MAR 10; "(U) RUSSIA: Militants Carry Out Further 'Acts of Sabotage' In Dagestan, Ingushetia;" (U)
8 (U) OSC; SAP20091118428004, 18 Nov 09; "(U) India: Suspected ULFA Militants Blow Up Fuel Train in Assam;" (U)
9 (U) Worldwide Incidents Tracking System; http://wits.nctc.gov; 31 March 2010; (U)
10 (U) Classified document: DHS Special Assessment; 12 December 2005; "(U//FOUO)
11 (U) Statement of TSA Office of Information Technology; 25 August 2010; (U//FOUO).
12 (U) cbsnews.com; "Virus Disrupts Train Signals," 21August 2003; (U)
13 (U) TSOC E-mail Report; Incident Trend of Note; 16 May 2009; (U//FOUO)
14 (U) MBTA Transit Police Department Informational Advisory; 16 March 2009; (U)