Safeguarding Rail Infrastructure During Mass Gatherings

SCOPE: This product is intended to highlight attacks against rail systems, particularly during mass gatherings for special events. Foreign terrorist organizations (FTOs) remain interested in attacking rail assets, and global threat actors continue to use sabotage tactics[a] against transit targets, which might further inspire violence against them.

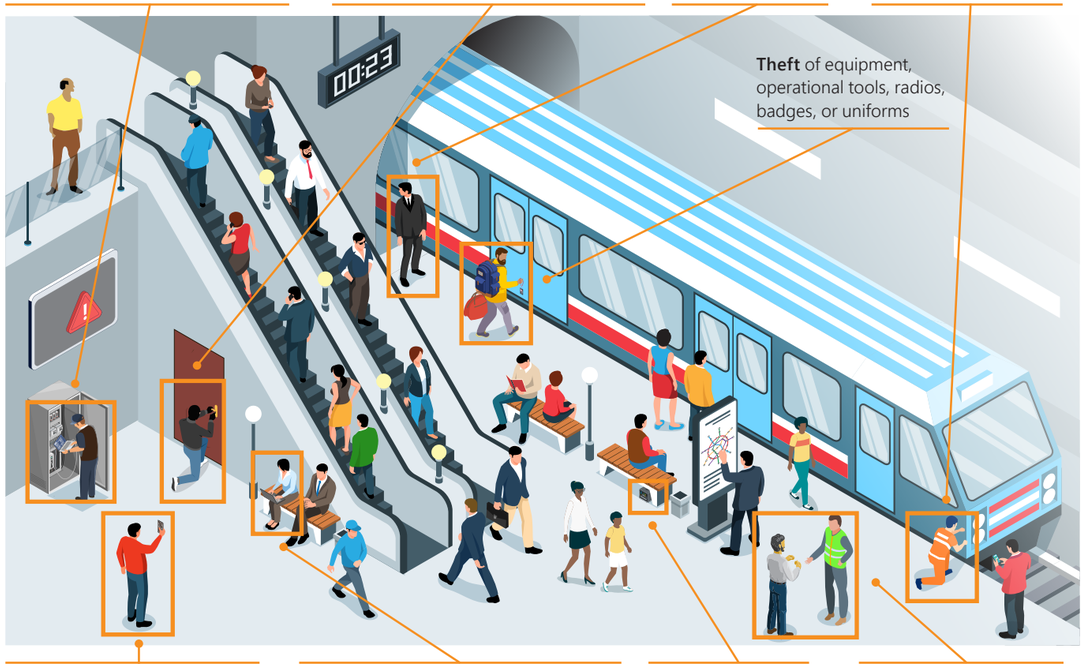
Terrorists may perceive rail assets, such as mass transit and freight rail, as attractive targets. Rail lines in metro areas are vulnerable because they have dense crowds of riders with minimal passenger screening requirements and extensive infrastructure networks with minimal security. Rail lines in more remote areas may experience slower emergency response times from first responders because of distance from them as well as thousands of miles of unprotected rails. Physical or cyber threats to rail assets can impact operations and public safety, particularly when operating above normal capacity, such as during a mass gathering. Common rail attack methods include physical attacks or disruption tactics, such arson, shunts, track obstructions, and sabotage of brake hoses, signal systems, or train car couplers.

As recently as February 2026, a pro-ISIS group claimed a suicide attack against a rail station in Moscow that killed one police officer and wounded two others. FTOs continue to attempt to inspire supporters to violence through terrorist publications. Violent extremists, driven by sociopolitical grievances, may seek to replicate tactics used in past attacks, which could cause cascading consequences to critical infrastructure that falls across different and several jurisdictions. Although some of the following examples are not examples of terrorism, the tactics, techniques, and procedures (TTPs) used by nefarious actors could be replicated by FTOs, which have demonstrated interest in attacking rail infrastructure.

- In February, one or more suspected anarchist violent extremists burned cables and severed a steel cable on railway lines serving the 2026 Milan-Cortina Winter Olympic venues. The incident, which caused minor disruption, prompted strengthened counterterrorism measures, including increased patrols and technical monitoring around Olympic venues.
- Before the 2024 Paris Olympics, France's high-speed rail network was subjected to coordinated disruptions, including track fires, cut fiber-optic cables that relay information to conductors, signal box cutting, and fire damage to signal boxes that connect Paris to other cities. Nearly 800,000 passengers were affected by the attacks.
- In 2023, a coordinated radio-stop attack[b] through VHF (very high frequency) disrupted more than 20 trains in Poland. The attack triggered the trains' emergency brakes and could have frozen transit for hours, which would have created a massive security bottleneck and a potential crowd control scenario.
- A cyber attack in 2022 that targeted a subcontractor for the Danish State Railways paralyzed local and regional rail lines for hours. The attack was suspected of being a dry run for a ransomware attack, but trains were shut down as a precaution to prevent malware from spreading to the control system.

Potential indicators[c]

Mobilization to violence often includes observable behavioral indicators, such as surveillance, training, recruitment, and rehearsal. Additional indicators can be found in the NCTC-DHS-FBI US Violent Extremist Mobilization Indicators booklet.



Reports of individuals attempting to **interfere with or disrupt regular railroad operations**; observed **cyber attacks** or successful **network penetrations**

Physical threats or intrusions, such as unusual **loitering** or **entry attempts** by unauthorized personnel, or **trespassing** and **vandalism** in and around the facility, which may indicate casing and perimeter security tests

Employees seeking **physical or digital access** beyond their normal duties

Tampering with railroad tracks, crossings, or other rail assets and infrastructure

Theft of equipment, operational tools, radios, badges, or uniforms

Photographic or video surveillance, including drone or small unmanned aircraft systems (UAS) operating near rail facilities, staff, or systems, or employees who bring unauthorized cameras, tools, or software into the workplace

Explicit or implied **threats to facilities or personnel**, which—communicated in person or online—may identify specific attack-planning details, including targets, time frames, and participant roles; **online posts** by individuals noting their intent to commit violence, or a direct threat with justification for action

Presence of **unusual wires, cables, electrical equipment, or devices** near railroad tracks

Indications that outsiders are trying to elicit information from a rail-related organization's staff, including individuals contacting employees with **requests for proprietary or sensitive information**

[a]Sabotage tactics intentionally injure, interfere with, obstruct, infect, or destroy rail system or assets.

[b]A radio-stop attack involves using radio-frequency technology to maliciously interfere with, disrupt, or control electronic systems.

[c]The totality of behavioral indicators and other relevant circumstances should be evaluated when considering law enforcement response or action.

NCTC-JFRT-2026-07690

16 APRIL 2026
AUTHORED BY NCTC, DHS, FBI

Safeguarding Rail Infrastructure During Mass Gatherings *(continued)*

Considerations

The following may help public safety, rail, and mass transit officials plan for potential threats or attacks against rail assets surrounding special events.

- **Stations-as-Stadiums:** Throughout events, stations may experience crowd surges multiple times per day. Treating high-density stations as de facto event venues with security screening and medical triage units could enhance response efforts.
- **Planning:** Pre-positioning equipment or repair materials near key infrastructure points can provide critical readiness capability and rapid response. Consider rail lines that share routes with hazardous materials (HAZMAT), and have appropriate HAZMAT resources pre-staged or available.
- **Interoperable Communications:** Test radios and secure communications to ensure access to real-time incident information sharing. In some cases, cellular network coverage in or around transit environments, including tunnels or rural areas, may be unreliable. Ensuring that police, fire, and EMS operations are operating on interoperable systems and have access to backup communications may help with safety and response. For agencies near the US-Canada or US-Mexico borders, communication lag may be a risk. Ensure interoperable communications through Joint Operations Centers or designated security agencies.
- **Special Event Support:** Before and during mass gatherings, use technology, including UAS, to identify potential suspicious activities and enable rapid response. A dedicated command center, such as a real-time crime center or fusion center, to identify and vet suspicious activity or threats and information sharing promotes multi-jurisdictional collaboration and enhanced response capabilities. Ensure that relationships between public safety, transit/rail agencies, and event/venue staff are established before events.
- **Multi-jurisdictional Considerations:** Rail stations or lines often lie within or across multiple jurisdictions, which may require state and local response to calls for service. Developing mutual aid agreements or standard protocols between responding jurisdictions can help clarify roles, enhance capabilities, and provide additional personnel, equipment, or resources, if needed.
- **Threat Awareness:** Staying aware of terrorist TTPs, including current and historic terrorist messaging promoting tactics against rail systems, can help mitigate potential threats. Be familiar with the range of resources, and participate in meetings, briefings, and information exchanges through state and local fusion centers and local FBI field offices to gain insights about the dynamic terrorist threat environment.
- **Collaboration with Rail Law Enforcement:** Understand the rail ownership in your jurisdiction, and know how to contact the relevant rail authorities. Railroad police are empowered by state statues and federal laws and regulations (48 USC 28101 and 49 CFR 207) to enforce state laws and protect people and property across the states in which railroad companies own, operate, and maintain property.
- **Cyber Security Mitigation:** Invest in measures to protect digital infrastructure, such as switching stations, signaling systems, automated control systems, dispatch operations, and public address systems, including display boards. Conduct routine cyber security audits, and enhance collaboration between cyber security and industry partners. Incorporate enhanced network defense practices, especially during periods of heightened internet traffic, such as mass gatherings. Stay alert for anomalous activity, and patch potential vulnerabilities, which can be mitigated through standard cyber hygiene.
- **Insider Threat Mitigation:** Witting or unwitting individuals who pose potential insider threats may exploit their access to critical systems, networks, facilities, or operations. Provide comprehensive training to employees, contractors, and volunteers. Training should cover essential security practices, thresholds for reporting suspicious activities, and insider threat awareness.
- **Public Awareness and Outreach:** Promote identification and reporting of suspicious activity. Use public messaging campaigns through social media platforms, websites, billboards, and transit resources, such as train cars, platforms, and stations.
- **Technology Integration:** Consider coordinated law enforcement UAS overwatch of railways and stations with designated no-fly areas for civilian UAS to ensure safety and security. Integrate available technology to the widest extent. Incorporate CCTV and use it regularly to ensure operational readiness.

Resources[d]

FBI's Rail Security Program has rail liaison agents in all FBI Field Offices who can assist law enforcement in intelligence matters pertaining to rail events, including investigations of rail-related incidents. To access this resource, email the FBI Rail Security Program team at FBI_NJTTF_RSP@ fbi.gov.

TSA manages the Transportation Security Operations Center, where rail owners/operators can report significant security concerns by calling 1-866-615-5150. TSA retains security incidents records for awareness and analysis, including threats to the mode of transportation, unauthorized access, suspicious activity, and theft of critical security items. Reported details should include reporter info, the threat source, affected assets, route details, incident descriptions, and involved parties.

Amtrak's Operation RAILSAFE is series of courses for first responders, railroad personnel, and transit agencies to improve passenger, infrastructure, and employee security.

NCTC-DHS-FBI Violent Extremist Mobilization Indicators and the Critical Infrastructure Sector

JCAT First Responder's Toolboxes provide information about terrorist tactics and response and mitigation considerations. These products can be found on JCAT's website, DHS's Homeland Security Information Network, or FBI's Law Enforcement Enterprise Portal.

- Awareness of Preoperational Surveillance Tactics Associated With Terrorism Offers Opportunities
- Large Public Gatherings Attractive Targets for Violent Extremists
- Evaluating and Responding to Violent Extremist Hoax Threats
- Railway Disruption Tactics: Threat Awareness, Detection, and Response Considerations
- Terrorist Insider Threat
- Rail-Safety Awareness for First Responders
- Complex Operating Environment—Mass Transit

[d]The materials listed illustrate the variety of offerings and should not be considered endorsements of the content offered.

NCTC-JFRT-2026-07690

16 APRIL 2026
AUTHORED BY NCTC, DHS, FBI

JCAT

JOINT COUNTERTERRORISM ASSESSMENT TEAM

PRODUCT FEEDBACK

Please use the link below to complete a short survey. Your feedback will help JCAT develop counterterrorism products that support the public safety and private sector community.

https://www.JCAT-url.com

For further information, please email JCAT
jcat@odni.gov

(U) The Joint Counterterrorism Assessment Team (JCAT) is a collaboration by NCTC, DHS, FBI, state, local, tribal, and territorial government personnel to improve information sharing and enhance public safety. The First Responder's Toolbox is an ad hoc, unclassified reference aid intended to promote counterterrorism coordination among federal, state, local, tribal, and territorial government authorities and partnerships with private sector officials in deterring, preventing, disrupting, and responding to terrorist attacks.