

# Information Sharing & Analysis Center

PUBLIC TRANSPORTATION  
& OVER THE ROAD BUS



## OVER-THE-ROAD-BUS INTELLIGENCE AWARENESS DAILY (OTRBIAD) REPORT

February 25, 2025

### SUSPICIOUS ACTIVITY & INCIDENT REPORTS

**Police: Philadelphia Man Arrested At Altoona Bus Station With Nearly \$45K Worth Of Meth**  
*WJAC, 2/24/2025*

[Pennsylvania] Police say a Philadelphia man was caught at an Altoona bus station with tens of thousands of dollars worth of suspected methamphetamine. Altoona police say authorities arrested 34-year-old Rashon Shariyf Shuler last Friday at the Greyhound bus station with approximately one pound of meth in his possession. Investigators noted that Shuler had an outstanding warrant out of Cumberland County. Police say the drugs found in his possession had an approximate street value of nearly \$45,000. <https://wjactv.com/news/local/police-philadelphia-man-arrested-altoona-bus-station-45k-worth-meth-drugs-dealer-blair-county-pennsylvania-wanted-warrant-greyhound-jail>

**MBTA Commuter Rail Train Collides With Car In Concord; Leaves 1 Hospitalized**  
*MassLive, 2/24/2025*

[Concord, Massachusetts] An MBTA commuter rail train collided with a car in Concord Sunday night, leaving a driver with minor injuries. The collision happened around 7 p.m. at the Conant Street crossing gate at "a low rate of speed," the Concord Fire Department said. The MBTA commuter rail train was headed west to Fitchburg. The sole occupant in the car had only minor injuries, the Concord Fire Department said. They were taken to Lahey Hospital & Medical Center in Burlington. At 7:53 p.m., the MBTA Commuter Rail posted on X, formerly Twitter, that the Fitchburg Line Train 2411 that was supposed to leave North Station at 6:15 p.m. Sunday was "terminated" after West Concord "due to a road vehicle on the right of way." <https://www.masslive.com/news/2025/02/mbta-commuter-rail-train-collides-with-car-in-concord-leaves-1-hospitalized.html>

### TERRORISM & EXTREMISM

**Explosive Devices Thrown at Russian Consulate in France**  
*Newsweek, 2/24/2025*

[France] Three explosive devices were thrown at the Russian Consulate in Marseille, France, on Monday, two detonating inside the consulate's perimeter, according to local police. No injuries were reported, but

NOT FOR PUBLIC DISSEMINATION



**HSIN-Intel**

Homeland Security  
Information Network  
Intelligence



# Information Sharing & Analysis Center

PUBLIC TRANSPORTATION  
& OVER THE ROAD BUS



the incident has heightened tensions between Moscow and Paris, and Russia has demanded a full investigation into what it described as an act of terrorism. The attack on the consulate comes on the third anniversary of Russia's full-scale invasion of Ukraine. While no group has claimed responsibility, the timing and nature of the attack have raised concerns about rising hostilities linked to the ongoing war. The Russian Embassy in Paris had previously requested increased security at the country's consulates in France, Russian media agency TASS reported. <https://www.newsweek.com/explosion-inside-russian-consulate-french-city-reports-2035112>

**ANALYST COMMENTARY:** On 24 February 2025, an unidentified individual threw two or three improvised incendiary devices at the Russian Consulate in Marseille, France. At least one of the devices exploded on contact on consulate grounds, and another device bounced off the consulate's outer walls and failed to detonate. No injuries were reported, and the extent of the damage is unclear. The suspect fled before law enforcement responded and has not been identified. Law enforcement safely disposed of the unexploded device, and media have reported that law enforcement told them the device was a Molotov cocktail housed in a plastic bottle, though they did not remark on the accelerant used. Historically, threat actors have used improvised incendiary devices and fire as a weapon against critical infrastructure in the U.S., and the number of incidents in U.S. metropolitan cities where fire was used as a weapon increased by almost 57 percent from 2019 to 2020. During the same time frame, the use of improvised incendiary devices also increased substantially, with government buildings seeing a 210 percent increase, commercial facilities seeing a 113 percent increase, and critical infrastructure sites seeing a 141 percent increase. These numbers may have been somewhat inflated during the COVID-19 pandemic due to the large number of violent protests in U.S. cities at the time, many of which resulted in widespread acts of arson. For example, over a three-day period spanning from 27 May 2020 to 30 May 2020, 164 separate arson incidents were reported during protests in St. Paul, Minnesota. Over 200 structures were damaged by the fires, and some 17 people were later charged for their role in causing arson related damages at 11 properties, and most of those charged had either livestreamed or posted social media videos of them starting the fires. A Cybersecurity and Infrastructure Security Agency (CISA) action guide regarding the use of fire as a weapon and mitigation techniques can be found here: [https://www.cisa.gov/sites/default/files/2024-08/fire-as-a-weapon-action-guide\\_08-30-2024\\_508.pdf](https://www.cisa.gov/sites/default/files/2024-08/fire-as-a-weapon-action-guide_08-30-2024_508.pdf)

## A Threshold Moment in Terrorist Trends and Targeting?

*War on the Rocks, 2/24/2025*

This year began alarmingly with the terrorist attack on New Orleans' famed Bourbon Street. The assailant, Shamsud-Din Jabbar, a U.S. Army veteran with a troubled past, claimed to have joined the self-proclaimed Islamic State in 2024 and displayed its flag in the truck he used to mow down and kill 14 people and injure some three dozen others. That incident tragically wiped away any illusion that the

### NOT FOR PUBLIC DISSEMINATION

Timely reporting to the **TSA Transportation Security Operations Center** is essential. Reports are made by telephone at **866-615- 5150** and by e-mail at **TSOC.ST@tsa.dhs.gov**.



**HSIN-Intel**

Homeland Security  
Information Network  
Intelligence



# Information Sharing & Analysis Center

PUBLIC TRANSPORTATION  
& OVER THE ROAD BUS



threat of terrorism has passed and that groups like the Islamic State, which were more active a decade ago, had been completely deprived of their capacity to continue to inspire attacks in the United States. A hard look at recent terrorist trends and targeting highlights how we are in fact at a critical turning point in global terrorism. Terrorists are embracing new tactics and seeking different target sets in order to overcome the mostly effective countermeasures and security procedures that have thwarted their attack plans in the past. <https://warontherocks.com/2025/02/a-threshold-moment-in-terrorist-trends-and-targeting/>

## SECURITY & SAFETY AWARENESS

### 21-Year-Old Accused Of Planning 'Mass Casualty Attack' On Texas Police

NBC, 2/25/2025

[Texas] Authorities in Texas said they thwarted a "mass casualty attack" on law enforcement and arrested a 21-year-old on charges of making terroristic threats. Corpus Christi police officers arrested Seth "Andrea" Gregori on state charges Monday morning, the department said in a Facebook post. The threats were allegedly made against the Corpus Christi Police Department. Gregori allegedly "planned an attack on police similar to the 2016 Dallas ambush," FBI Houston said in a post on X. Five Dallas police officers were killed in the ambush-style attack. The shooter in the 2016 attack, Micah Xavier Johnson, told a hostage negotiator that he "wanted to kill white people, especially white officers," authorities said. The Army veteran was killed after authorities detonated a bomb following several hours of negotiations. <https://www.nbcnews.com/news/us-news/21-year-old-accused-planning-mass-casualty-attack-texas-police-rcna193621>

**ANALYST COMMENTARY:** On 24 February 2025, law enforcement in Texas arrested a 21-year-old man for planning a mass casualty attack against police following a federal investigation. The suspect's motive and plans are unclear; however, the Federal Bureau of Investigation (FBI) claimed the suspect was planning "an attack on police similar to the 2016 Dallas ambush." During that incident, a 25-year-old Army veteran and Black nationalist with a history of espousing violent and racist rhetoric shot 14 police officers, killing five, with an AK-pattern rifle during multiple short, ambush style engagements while the officers were on duty at a demonstration protesting police brutality in Dallas, Texas. The attacker began his attack at approximately 9 p.m. while the protest was closing down, and remained mobile for most of the shootings, which challenged the law enforcement response because police believed there were multiple shooters. The shooter was eventually pursued into a building and cornered, at which time he shouted "Black supremacy! Black liberation!" and shot at officers again. After two hours of failed negotiations, law enforcement used a bomb strapped to a bomb-disposal remote controlled robot to kill the suspect around 2:30 a.m. and ended the standoff. According to data compiled by the FBI, attacks against police officers in the U.S. reached a 10-year high in 2023,

### NOT FOR PUBLIC DISSEMINATION

Timely reporting to the **TSA Transportation Security Operations Center** is essential. Reports are made by telephone at **866-615- 5150** and by e-mail at **TSOC.ST@tsa.dhs.gov**.



**HSIN-Intel**

Homeland Security  
Information Network  
Intelligence





# Information Sharing & Analysis Center

PUBLIC TRANSPORTATION  
& OVER THE ROAD BUS



with more than 79,000 officer attacks reported, 466 of which involved the use of firearms, and 60 of which resulted in officer fatalities.

## **NYPD Subway Crackdown Aimed at Finding Criminal Offenders**

*Officer.com, 2/24/2025*

[New York] A homeless man accused of shoplifting 17 times at the same Queens Duane Reade and menacing a security guard was back behind bars after police took him into custody for stretching out across several subway seats, the Daily News has learned. The NYPD said the Feb. 7 arrest of Luis Caballero, 36, is an example of how enforcing NYC Transit rules maintains order in the subway system and often leads to the arrest of offenders wanted for crimes. Critics argue, though, that such crackdowns invariably ensnare the poor and the homeless in the criminal justice system, such as when a warrant is issued because someone with an initial summons doesn't show up in court or pay the required fine. Caballero's bust happened eight days after Police Commissioner Jessica Tisch's announcement that the NYPD will make sure straphangers don't violate rules that bother other riders, such as taking up more than one seat, smoking and drinking alcohol. Tisch said the initiative "is designed to address the surge of random acts of violence we're seeing in the subways." <https://www.officer.com/command-hq/news/55270229/new-york-police-department-quality-of-life-new-york-city-subway-crackdown-aimed-at-finding-criminal-offenders>

## **OMNY Fare Readers Keep Falling Off Mounts On MTA Buses**

*Gothamist, 2/23/2025*

[New York] OMNY readers used to collect fares on MTA buses keep falling off their mounts, forcing the agency to spend \$4.5 million to fix the problem, according to contract documents published Friday. The problem persisted for years while transit officials traded blame with representatives from Cubic, the company contracted to install and oversee the OMNY system, the documents show. "In January 2021, cracks were found affecting a large number of the mounting brackets resulting in the bus validators falling off their mounts," the MTA documents said. "There was a dispute between MTA and Cubic as to whether the failure of the brackets was a design defect or caused by MTA's maintenance of the brackets." The MTA board is slated to approve the expenditure to fix the mounts on Wednesday. The agreement requires Cubic to install new mounting brackets for the 11,359 tap-to-pay readers in place on the MTA's fleet of buses. The issue is the latest mishap in the MTA's rollout of OMNY. The MTA inked a \$573 million contract with Cubic to install the system in 2017 with plans to fully phase out the MetroCard in 2023. <https://gothamist.com/news/omny-fare-readers-keep-falling-off-mounts-on-mta-buses>

### **NOT FOR PUBLIC DISSEMINATION**

Timely reporting to the **TSA Transportation Security Operations Center** is essential. Reports are made by telephone at **866-615- 5150** and by e-mail at **TSOC.ST@tsa.dhs.gov**.



**HSIN-Intel**

Homeland Security  
Information Network  
Intelligence



# Information Sharing & Analysis Center

PUBLIC TRANSPORTATION  
& OVER THE ROAD BUS



## **Montreal's Metro Struggles To Cope With Growing Homelessness Crisis** *CBC, 2/24/2025*

[Montreal, Canada] As the evening cold set in, Lindy Trapper and three friends spread a blanket on a platform overlooking the tracks at Villa-Maria Metro, in Montreal's west end. Soon after, two intervention workers told them to leave. They were escorted up to the subway entrance, but without any clear options, stayed inside. "I hang around in the Metro until it closes, and then I have to look for somewhere to sleep," said Trapper, a Cree man from Mistissini, Que. When the Metro does close, Trapper said he often spends the night in a storefront entrance, where he can escape the worst of the wind. In the morning, he returns to the Metro. Similar situations are unfolding across the subway system, where people without a place to stay seek reprieve from the cold and snow. Reports of disturbances in the Metro system, drug usage and concerns from riders about their safety have all surged since the pandemic. <https://www.cbc.ca/news/canada/montreal/montreal-metro-homeless-1.7465094>

## **AI Offers Benefits, Risks To Public Transit: Urban Institute Researcher** *Smart Cities Dive, 2/24/2025*

Artificial intelligence and machine learning technologies could reduce safety risks and increase operational efficiency while improving riders' experience with public transportation, says a Feb. 5 blog post by the Urban Institute's Lindiwe Rennert, a senior research associate in the Housing and Communities Division. Some transit agencies are already using these technologies to monitor stations, tracks and roadways for dangerous conditions and to better predict expected passenger use to avoid overcrowding. AI and machine learning can also help to identify bus or train maintenance issues before they result in a breakdown. But AI and machine learning come with concerns around equity, discrimination and biases, along with the risks of hacking and misuse of personal data, the post states. <https://www.smartcitiesdive.com/news/ai-machine-learning-public-transit-benefits-risks-urban-institute/740734/>

## **Hill Weighs Expanding Ban on Foreign Nationals at DoE Labs** *MeriTalk, 2/21/2025*

Lawmakers on Capitol Hill are considering expanding a ban on preventing all foreign-born nationals from adversarial nations from working in the Department of Energy's (DoE) 17 national labs, citing risks of espionage. During a Feb. 20 hearing of the Senate Committee on Energy and Natural Resources, legislators and witnesses agreed on the need for increased cybersecurity protections to counter DoE staffers who may be conducting espionage and gaining access to sensitive information on technological advancements critical to U.S. national security. "From the Manhattan Project to cutting edge AI [artificial intelligence] research, DoE's national labs have pushed the boundaries of innovation and strengthened our national security, but for those very same reasons, they've also become a prime target for espionage," committee Chairman Mike Lee, R-Utah, in opening statements. "For years, the Chinese

**NOT FOR PUBLIC DISSEMINATION**

Timely reporting to the **TSA Transportation Security Operations Center** is essential. Reports are made by telephone at **866-615- 5150** and by e-mail at **TSOC.ST@tsa.dhs.gov**.



**HSIN-Intel**

Homeland Security  
Information Network  
Intelligence



# Information Sharing & Analysis Center

PUBLIC TRANSPORTATION  
& OVER THE ROAD BUS



Communist Party (CCP) has worked to infiltrate our national labs, targeting top scientists and siphoning off American research to fuel China's military ambitions," he said. <https://www.meritalk.com/articles/hill-weighs-expanding-ban-on-foreign-nationals-at-doe-labs/>

## CYBERSECURITY

### **Snake Keylogger Variant Hits Windows, Steals Data via Telegram Bots**

*HackRead, 2/18/2025*

Cybersecurity researchers at FortiGuard Labs have discovered a new variant of the Snake Keylogger, also known as the 404 Keylogger, targeting Windows users. As per their research, shared with Hackread.com, this malware is designated Autolt/Injector.GTY!tr, and has been linked to over 280 million blocked infection attempts globally, primarily concentrated in China, Turkey, Indonesia, Taiwan, and Spain. Researchers note that this Snake Keylogger variant typically spreads through phishing emails containing malicious attachments or links. It targets popular web browsers like Chrome, Edge, and Firefox, stealing sensitive information such as credentials and data by logging keystrokes, capturing credentials, and monitoring the clipboard. The stolen data is then exfiltrated to its command-and-control (C2) server via email (SMTP) and Telegram bots. According to FortiGuard Labs' technical report, the malware employs Autolt, a scripting language frequently used for Windows automation, to deliver and execute its malicious payload. <https://hackread.com/snake-keylogger-variant-windows-data-telegram-bots/>

**ANALYST COMMENTARY:** Autolt is a technique that malware authors are implementing because it can produce isolated executables that avoid detection by antivirus software. By injecting its payload into a Windows process, such as RegSvcs.exe, the malware blends in with regular system activity. The exfiltration of data using Telegram and SMTP points to a move away from a single command-and-control server and toward, decentralized data theft techniques. Dropping ageless.exe in %Local\_AppData%\supergroup and ensuring execution via ageless.vbs in the Startup folder means the malware remains active even after system reboots. This is a traditional method of low-privilege persistence that does not employ UAC prompts that could warn users. Because Autolt-compilation adds obfuscation layers, businesses should concentrate on behavioral anomaly detection for mitigation rather than just using signature-based security. Such threats can be identified with Endpoint Detection and Response (EDR) technologies that keep an eye on process injection and startup entries. The infection can be reduced by preventing Autolt-based scripts from running in unapproved environments and limiting unauthorized programs' access to Telegram and SMTP connections. User education on email security and attachment management is still a vital first line of defense against the widespread propagation of phishing.

### NOT FOR PUBLIC DISSEMINATION

#### \*\*\* FAIR USE NOTICE \*\*\*

This message contains copyrighted material whose use has not been specifically authorized by the copyright owner. The OTRB ISAC is providing this report to ISAC members who have expressed a prior interest in receiving information to advance their understanding of threat activities in the interest of protecting the national infrastructure of the United States. We believe that this constitutes a 'fair use' of the copyrighted material as provided for in section 107 of the U.S. Copyright Law. If you wish to use this copyrighted material for purposes of your own that go beyond 'fair use,' you must obtain permission from the copyright owner. For questions regarding this document, please contact the OTRB ISAC: 1-877-847-5510 or email [mcanalyst@motorcoachisac.org](mailto:mcanalyst@motorcoachisac.org)