

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION
& OVER THE ROAD BUS



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

February 12, 2025

SUSPICIOUS ACTIVITY & INCIDENT REPORTS

Two Slashed, Including MTA Security Guard, In Separate NYC Subway Attacks

New York Daily News, 2/10/2025

[New York] Two people — including a security guard — were mercilessly slashed Monday in disturbing subway attacks that erupted just minutes apart in Manhattan and Brooklyn, police sources said. In the first incident, a security guard contracted by the MTA at the 86th St. station on the Upper East Side confronted a man sneaking onto the downtown platform of the Nos. 4, 5, and 6 trains around 6:25 p.m., sources said. The guard tried to stop the fare evader, who became irate and pulled out a boxcutter, slashing the guard across the face. Medics took the wounded security guard to New York-Presbyterian Hospital Weill Cornell, where he was in stable condition. ... About a half hour later, two men argued on a Canarsie-bound L train, police said. As the train rumbled toward the Wilson Ave. station in Bushwick, one of the men pulled out a blade and slashed the 30-year-old man he was arguing with.

<https://www.nydailynews.com/2025/02/10/two-slashed-including-mta-security-guard-in-separate-nyc-subway-attacks/>

1 Dead And 25 Injured After A High-Speed Train And A Truck Collide In Germany

Associated Press, 2/11/2025

[Germany] A collision between a high-speed train and a truck on the outskirts of the German city of Hamburg left one person dead and 25 injured, six of them seriously, police said. The ICE train had 291 people on board at the time of the collision on Tuesday with a truck that was loaded with rails. Police said the uninjured passengers were evacuated and taken to a nearby station by bus. A 55-year-old passenger died at the scene. The train rammed the truck on a crossing and windows in cars at the front of the train shattered, German news agency dpa reported, citing a witness. The truck's load was strewn around the accident site. It wasn't immediately clear what led to the accident. The truck driver was taken in for questioning.

<https://apnews.com/article/germany-train-accident-truck-injuries-12e3c321ddff9caa3d5cf34495a320f4>

NOT FOR PUBLIC DISSEMINATION



HSIN-Intel

Homeland Security
Information Network
Intelligence



Information Sharing & Analysis Center

PUBLIC TRANSPORTATION
& OVER THE ROAD BUS



Large Fire Erupts Near El Paso, Texas, International Airport, Injuring 5 *ABC, 2/11/2025*

[El Paso, Texas] A fire broke out at a transportation center next to the international airport in El Paso, Texas, on Tuesday, injuring five people and sending a large tower of black smoke billowing over the city on the U.S.-Mexico border. Authorities did not immediately say what caused the fire at Sun Metro Bicentennial Council Transit Operations Center. More than 100 firefighters responded to the blaze, said El Paso Fire Department Deputy Chief Robert Arvizu. He said he did not immediately know how many people were inside the building, whose walls and roof caved in. Authorities said they had the fire under control by midafternoon. The fire did not disrupt flights at El Paso International Airport, said El Paso city spokesperson Laura Cruz Acosta. <https://abcnews.go.com/US/wireStory/large-fire-erupts-el-paso-texas-international-airport-118715133#:~:text=EL%20PASO%2C%20Texas%20--%20A%20fire%20broke%20out,billowing%20over%20the%20city%20on%20the%20U.S.-Mexico%20border>.

ANALYST COMMENTARY: On 11 February 2025 at approximately 1 p.m. local time, a vehicle explosion occurred in a bus maintenance garage at the Sun Metro Operations Center in El Paso, Texas. The cause of the explosion is unclear, though authorities have said they do not believe it was caused by the use of a manufactured explosive. Authorities have not remarked on what kind of vehicle initially exploded; however, Sun Metro's vehicle fleet runs on compressed natural gas which is extremely flammable. Following the initial explosion, a large fire broke out and over 48 firefighting units and 100 firefighters responded to the scene. The fire was extinguished at approximately 4:40 p.m., and seven people were assessed for injuries, including four who were transported to the hospital. Two of those in the hospital are in reportedly critical condition, and one is in serious condition. The fire caused significant damage to the structure, and the roof and multiple walls have reportedly collapsed. The degradation of the operations center has disrupted transit operations and Sun Metro has said they will be adjusting their bus routes for at least a week to their "Sunday/Holiday" limited schedule. The El Paso Fire Department is conducting an investigation into the fire.

RTD Bus Slides Off Icy Road In Westminster *Denver Post, 2/12/2025*

[Westminster, Colorado] A Regional Transportation District bus carrying six passengers slid off the road Wednesday morning in Westminster amid the wave of snowy, icy weather, police said. The early morning crash happened as the bus was headed to the RTD Park and Ride near U.S. 36 and Sheridan Boulevard, the Westminster Police Department said at 6:52 a.m. on X. Police officials said no one was injured in the crash and all six passengers were safely evacuated onto a new bus. All but one lane of U.S. 36 is closed for the crash cleanup and investigation, police said. <https://www.denverpost.com/2025/02/12/crash-rtd-bus-slides-off-road-westminster/>

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



Woman Struck With Pipe, Robbed Of Cell Phone At Hayward BART Station

East Bay Times, 2/11/2025

[San Francisco, California] An 18-year-old woman was struck with a metal pipe and robbed of her cell phone Monday evening at the South Hayward BART Station, officials said. A suspect was later arrested. The violent attack happened about 6:30 p.m. Monday on the station platform. Authorities said the woman, a Hayward resident, was struck at least once with a metal pipe by a 42-year-old man who robbed her of her cell phone and fled on foot. Authorities said there is no indication the suspect knew the woman. The woman was able to contact the BART police dispatch center and responding officers arrested the suspect within a few minutes. The cell phone was recovered. ... The suspect, who has addresses in both Oakland and San Leandro, was booked at Santa Rita Jail on suspicion of assault with a deadly weapon other than a firearm and robbery. He was being held in lieu of \$195,000 bail and is scheduled to be arraigned in court on Thursday. <https://www.eastbaytimes.com/2025/02/11/woman-struck-with-pipe-robbed-of-cell-phone-at-hayward-bart-station/>

Photos Show Suspects Wanted For Battering, Robbing Person On CTA Red Line Train

FOX 32, 2/10/2025

[Chicago, Illinois] The Chicago Police Department is searching for a group of suspects who allegedly battered and robbed a man on a CTA train earlier this month. The incident occurred in the 200 block of West 63rd Street around 3:55 a.m. on Feb. 3, when three offenders approached a passenger on a CTA Red Line train, battered him and robbed him of his personal property. The offenders are described as two African American males and one Latino male, between the ages of 15 and 20. Their heights and weights vary, according to police. <https://www.fox32chicago.com/news/cta-red-line-train-robbery-englewood>

TERRORISM & EXTREMISM

UN Security Council Raises Alarm Over Rising IS-K Threat From Afghanistan

Voice of America, 2/10/2025

United Nations counterterrorism officials warned during a Security Council meeting Monday that an Islamic State affiliate in Afghanistan remains a significant threat to regional and global security. The discussion centered on the threat posed by Islamic State, also known as Daesh, and its regional offshoots to international peace and security. The Afghan-based Islamic State-Khorasan (IS-K) was highlighted as one of the “most dangerous branches” of the transnational terrorist group. It has carried out repeated high-profile attacks targeting Afghan civilians and members of the country’s de facto Taliban rulers. “ISIL-Khorasan has continued to pose a significant threat in Afghanistan, the region and beyond,” Vladimir Voronkov, U.N. undersecretary-general for counterterrorism, told the meeting, using another acronym for IS-K. He stated that IS-K supporters had plotted attacks in Europe and were actively seeking to recruit

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



individuals from Central Asian countries. <https://www.voanews.com/a/un-security-council-raises-alarm-over-rising-is-k-threat-from-afghanistan/7969985.html>

ANALYST COMMENTARY: The Islamic State in Iraq and Syria-Khorasan (ISIS-K, aka IS-KP, ISK) is an Islamic State Group (ISG) regional affiliate located primarily in Afghanistan and Pakistan, the area of which was historically known as the Khorasan. The group was officially established in Afghanistan in 2015, and most of its original members were heavily recruited to ISIS-K from other preexisting terrorist and militant groups in the region. While ISIS-K's primary goal is to achieve dominance over the Khorasan region and establish a caliphate there that adheres to a strict version of sharia law, they have also inspired and perpetrated attacks well outside of their territorial boundaries to garner attention and notoriety. In addition, their affiliate media arm, the al-Azaim Media Foundation, publishes a significant amount of digital propaganda like the popular terrorist magazine Voice of Khorasan (VoK), which often calls for sympathizers to attack against western nations and provides readers with instructional guides for manufacturing explosives and recommends tactics for carrying out attacks against civilian populations in Western nations. Following the vehicle ramming attack in New Orleans on 1 January 2025, the al-Azaim Media Foundation produced propaganda that "advocated for lone-actor attacks on a variety of celebrations and public events in the U.S. and Europe, and, referencing the New Orleans attack, urged, 'don't wait for a new year to take action'." The al-Azaim Media Foundation is quite active and generally produces weekly content. Most recently, on 30 January 2025, the al-Azaim Media Foundation published two digital posters praising the ISG in general, and glorifying those who carry out terrorist attacks in furtherance of ISG ideology. Prior to that, on 26 January 2025, they published the 43rd issue of the VoK magazine which was pushing recruitment efforts in Pakistan, Iran, and Afghanistan; encouraging members and sympathizers to use Telegram for communications instead of other messaging apps; and asking for financial support via the Monero app.

SECURITY & SAFETY AWARENESS

BART Running Out Of Emergency Funding, Facing Potential Shut Down

KRON 4, 2/11/2025

[San Francisco, California] Bay Area Rapid Transit has announced that the transit system is facing a "fiscal cliff" and may run out of emergency funds in 2026. BART believes the effects of the COVID-19 pandemic "decimated" transit ridership. After the pandemic, remote work has become a norm for many. According to BART, prior to the pandemic money from passenger fares and parking fees covered nearly 70% of the cost to run BART service and now only 25% of operating costs are covered by fares. The Bay Area has the highest work-from-home rates in the nation, according to BART. At the beginning of the pandemic, BART received nearly \$2 billion in federal, state and regional emergency assistance to keep trains running.

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



However, the funding is set to run out by spring 2026. <https://www.kron4.com/news/bay-area/bart-facing-fiscal-cliff-could-run-out-of-money-next-year/>

MTA Launches Pilot Program To Connect Deaf Riders With ASL Interpreters *6sqft, 2/11/2025*

[New York] Navigating the New York City subway system got a little easier for riders with hearing difficulties. The Metropolitan Transportation Authority on Monday announced a pilot program that instantly connects commuters who are deaf or hard of hearing with American Sign Language (ASL) interpreters while using the transit system. Through the Convo Access app, riders can connect with a live interpreter to communicate with MTA employees about service changes, payments, or any transit-related questions. The pilot, free for all customers, was first deployed at Penn Station, Times Square, and Port Authority. These locations saw a 94 percent activation rate, with users reporting improved personal connections and more natural interactions with transit staff. <https://www.6sqft.com/mta-launches-pilot-program-to-connect-deaf-riders-with-asl-interpreters/>

Merrimack Valley Transit First In State To Be Permanently Fare-Free *Boston.com, 2/11/2025*

[Merrimack Valley, Massachusetts] Merrimack Valley Transit, which serves 16 communities, is now permanently free for riders following an almost three year pilot, making the agency the first in the state to go completely fare-free, the agency announced. The Merrimack Valley Transit's advisory board voted 15-0, with one abstention, to adopt the fare-free policy permanently. In a press release, the transit agency said the decision came from reviewing the business analysis of the fare-free program. "Since transportation is the key to everything, the positive impact of fare-free buses has broad reaching impact across all sectors," Merrimack Valley Transit, or MeVa, said. <https://www.boston.com/news/local-news/2025/02/10/merrimack-valley-transit-first-in-state-to-be-permanently-fare-free/>

CYBERSECURITY

University Site Cloned To Evade Ad Detection Distributes Fake Cisco Installer *Malwarebytes, 2/5/2025*

There is a constant "cat and mouse" game between defenders and attackers, the latter trying to outsmart and get a head start on the former. In the context of online advertising, this involves creating fake identities or using stolen ones to push out malicious ads. An attacker not only needs to evade detection but also create a lure that will be convincing to most people. In this blog post, we focus on what malvertisers use in almost all of their campaigns, namely decoys also known as "white pages" in order to fool the advertising entity. The particular case is a malicious Google ad for Cisco AnyConnect, a

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



tool often used by employees to remotely connect to company networks, but also by universities. In fact, we found that threat actors were using the name of a German university to create a fake website designed not to fool actual victims, but rather to bypass detection from security systems. To be sure, victims were part of the overall scheme, but they were instead redirected to a lookalike Cisco site linking to a malicious installer containing the NetSupport RAT remote access Trojan.

<https://www.malwarebytes.com/blog/news/2025/02/university-site-cloned-to-evade-ad-detection-distributes-fake-cisco-installer>

ANALYST COMMENTARY: Threat actors are blending into legitimate environments by using AI-generated white pages and content published or stolen from websites to escape detection. The attacks that happened on Google's ad ecosystem flag the difficulties of enforcing safety in environments that are saturated with ad content. This problem raises the question of how vigilant the users have to be: search ads (one word ads) are still a common attack vector, particularly for software downloads. Search ads are paid advertisements that appear at the top of search engine results when users look up specific keywords. Companies bid on these keywords so their ads show up before organic (non-paid) results. These ads often resemble regular search results but are labeled as "Sponsored" or "Ad." Because search ads appear first and look legitimate, cybercriminals exploit them to distribute malware, phishing links, or scams. Organizations are encouraged to consider implementing ad-blocking solutions, restricting software installation permissions, and training their employees not to click on sponsored links when downloading sensitive applications. Defenders should focus on real-time monitoring of search ad abuse and integrate alerts for domain registration into their workflows for spotting and mitigating these threats at all possible speeds. Google and other platforms need to refine their screening of newly registered domains in ads, potentially flagging them for manual review before approval. Until then, this sort of attack will be a risk to corporate and university environments, especially where tools such as Cisco AnyConnect have become a staple.

*** 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

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

