

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION



Public Transportation ISAC Transit & Rail Intelligence Awareness Daily Report (TRIAD)

December 10, 2024

SUSPICIOUS ACTIVITY & INCIDENT REPORTS

Man Drunkenly Drove Car Onto LIRR Tracks, MTA Says

Long Island Press, 12/9/2024

[Long Island, New York] If you take the Hempstead, Ronkonkoma, Port Jefferson or Oyster Bay branches of the LIRR, chances are your commute yesterday was significantly delayed or even suspended entirely. A man, allegedly drunk, drove his car down the LIRR tracks and stopped there, potentially endangering the lives of the LIRR operators and passengers. Basilio Hidalgo, 40, from Brooklyn, drove his car onto the LIRR tracks near the Elmont-UBS Arena station and then drove down the tracks for a half mile to the Bellerose Station a little before 5 p.m. on Dec. 8, MTA officials say. The car's front two tires caught on fire, and had to be put out by the Floral Park Fire Department. Hidalgo's alleged drive significantly damaged the track, delayed the Ronkonkoma, Port Jefferson, and Oyster Bay branches, and entirely suspended service on the Hempstead Branch while an on-scene investigation took place. Hidalgo was arrested on the scene and immediately taken into police custody. His car was removed from the tracks at around 8:30 p.m., and service on the Hempstead branch was restored about ten minutes later.

<https://www.longislandpress.com/2024/12/09/dwi-car-lirr-tracks-mta/>

Woman Under The Influence Drove At 'High Rate Of Speed' Down Green Line Tracks, Say T Police

Boston.com, 12/9/2024

[Boston, Massachusetts] Police arrested a woman who drove onto MBTA Green Line tracks at a "high rate of speed" on Friday, officials said. At 2:30 a.m., the 27-year-old woman was allegedly driving while under the influence of alcohol in the Coolidge Corner area near Trader Joe's in Brookline, according to a statement from MBTA Transit Police. The woman then proceeded to speed down the MBTA tracks, police said. Authorities soon took her into custody and towed her vehicle from the scene. No injuries were reported. <https://www.boston.com/news/crime/2024/12/09/mbta-green-line-tracks-driver-under-influence-speeding-t-police/>

NOT FOR PUBLIC DISSEMINATION

*WARNING: THIS DOCUMENT IS UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). IT CONTAINS INFORMATION THAT MAY BE EXEMPT FROM PUBLIC RELEASE UNDER THE FREEDOM OF INFORMATION ACT (5 U.S.C. 552). IT IS TO BE CONTROLLED, STORED, HANDLED, TRANSMITTED, DISTRIBUTED, AND DISPOSED OF IN ACCORDANCE WITH DHS POLICY RELATING TO FOUO INFORMATION AND IS NOT TO BE RELEASED TO THE PUBLIC, THE MEDIA, OR OTHER PERSONNEL WHO DO NOT HAVE A VALID "NEED-TO-KNOW" WITHOUT PRIOR APPROVAL OF AN AUTHORIZED TSA OFFICIAL. NO PORTION OF THIS REPORT SHOULD BE FURNISHED TO THE MEDIA, EITHER IN WRITTEN OR VERBAL FORM. PLEASE REFER TO EACH DOCUMENT'S U//FOUO WARNING FOR FURTHER HANDLING INSTRUCTIONS THAT MAY APPLY.

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION



TERRORISM & EXTREMISM

3 Men Arrested In Germany Over Suspected Preparations For An Islamic Extremist Attack

Associated Press, 12/9/2024

[Germany] Two young men who sympathized with the Islamic State group and a suspected accomplice have been arrested in Germany for allegedly making preparations for an attack, authorities said Tuesday. The two German Lebanese brothers aged 15 and 20 from the southwestern city of Mannheim and a 22-year-old German Turkish man from the neighboring state of Hesse were arrested on Sunday, prosecutors and police said in a statement. The brothers are accused of preparing for an attack motivated by their religious ideology and "profound sympathy" for the Islamic State group, procuring among other things an assault rifle and ammunition. The weapon was found at the 22-year-old's home, the statement said. Investigators also found a balaclava, a protective vest and several knives, along with cellphones. A judge on Monday ordered the suspects kept in custody pending a possible indictment.

<https://apnews.com/article/germany-islamic-extremism-attack-plan-arrest-38ce3300bd7992a3253164d717579aad>

NC A Hotbed For Extremist Group's Activities, Expert Says

WRAL News, 12/10/2024

[North Carolina] Experts say North Carolina has become a hotbed for a growing extremist group's activities. WRAL started investigating the connection between the Sovereign Citizens movement and a recent deed fraud case we've reported on extensively in the last few months. ... "This group believes that they live outside the jurisdiction of, in this case, the United States of America, and as a result, they don't need to follow the US laws," explained Rachel Goldwasser. ... The instances of Sovereign Citizens becoming violent are rare, according to Goldwasser. "Unfortunately, these are all incidences where real people are getting hurt. Oftentimes it's law enforcement, although not always, and typically, it's when somebody is questioning the Sovereign Citizen on something." In August, a Sovereign Citizen killed a Dallas police officer then wounded two more responding officers. The Anti-Defamation League says it has been a record year for violent encounters between police and Sovereign Citizens. Goldwasser estimates there are over 300,000 Sovereign Citizens in the United States and their numbers seem to be growing every year. <https://www.wral.com/news/investigates/paper-terrorism-sovereign-citizens-north-carolina-december-2024/>

Ousted Syrian Leader Assad Flees To Moscow After Fall Of Damascus, Russian State Media Say

Associated Press, 12/8/2024

[Syria] Ousted Syrian leader Bashar Assad fled to Moscow and received asylum from his longtime ally, Russian media said Sunday, hours after a stunning rebel advance seized control of Damascus and ended his family's 50 years of iron rule. Thousands of Syrians poured into streets echoing with celebratory

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,
& SURFACE TRANSPORTATION



gunfire and waved the revolutionary flag in scenes that recalled the early days of the Arab Spring uprising, before a brutal crackdown and the rise of an insurgency plunged the country into a nearly 14-year civil war. The swiftly moving events raised questions about the future of the country and the wider region. <https://hosted.ap.org/article/816e538565d1ae47e016b5765b044d31/ousted-syrian-leader-assad-flees-moscow-after-fall>

ANALYST COMMENTARY: The collapse of Syrian President Bashar al-Assad's regime weakens the influence and control of several U.S. adversaries in the region but also carries substantial risk. Ultimately, the impact on regional and global security remains unclear due to the area's inherent instability and the numerous factions involved. A key concern is that militant elements within the Syrian rebel alliance will attempt to capitalize on the resulting power vacuum. During a visit to Japan, U.S. Secretary of Defense Lloyd Austin warned that "elements in the area, such as [Islamic State Group (ISG)], could try to take advantage of this opportunity and regain capability." In response to these concerns, the U.S. reportedly carried out more than 70 strikes in Syria on Sunday against ISG operatives and camps "to deny them the ability to easily resurge". Israel also targeted several sites linked to Iran and Syrian state forces and moved military assets into a demilitarized zone along its border with Syria. Israel said it would increase airstrikes on Syrian stores of advanced weaponry and maintain a 'limited' troop presence on the ground to contain spillover violence and stop weapons from falling "into the hands of extremists."

SECURITY & SAFETY AWARENESS

Suspect In Killing Of UnitedHealth Executive Brian Thompson Charged With Murder

Reuters, 12/10/2024

[Altoona, Pennsylvania] New York prosecutors filed a murder charge against the suspect in the killing of a UnitedHealth executive, a brazen shooting that set off a manhunt that culminated in his capture in Pennsylvania earlier on Monday. The action brought an end to a tense five-day manhunt for the suspected killer. The suspect, identified as Luigi Mangione, 26, was captured in Altoona, Pennsylvania, after he was spotted eating at a McDonald's by a customer and an employee who believed he resembled the gunman, officials said at a news conference. When approached by two police officers inside the McDonald's and asked if he had recently been in New York, Mangione began to shake and went quiet, one of the responding officers said at a press conference. He had been wearing a mask and sitting alone with a laptop and backpack. A search of the backpack at the police station turned up a black "ghost gun" - a firearm assembled from parts, making it untraceable - loaded with a magazine and a silencer. Pennsylvania authorities said the weapon, as well as clothing and a mask, were similar to those used by the killer. <https://www.reuters.com/world/us/investigators-question-man-connection-with-unitedhealth-exec-killing-reports-say-2024-12-09/>

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,
& SURFACE TRANSPORTATION



ANALYST COMMENTARY: On 9 December 2024, law enforcement in Altoona, Pennsylvania took 26-year-old Luigi Mangione into custody in connection with the murder of a healthcare insurance CEO last week. According to police, a witness telephoned them after observing Mangione eating at a McDonald's restaurant and claimed that Mangione looked like the photographs of the suspect that law enforcement nationwide had been circulating. Police took Mangione into custody without incident and discovered an illicit handgun, firearm suppressor, multiple fake IDs, and a three-page handwritten manifesto containing an admission to the murder among his possessions. It is unclear if the handgun recovered was the same weapon used in the murder. According to Newsweek, the manifesto "was heavily critical of the healthcare industry and warned that violence was the only answer to changing it," and in the manifesto, Mangione wrote that "these parasites had it coming." Multiple media outlets have also reported that Mangione had previously praised the Unabomber's actions, calling him an "extreme political revolutionary," and that Mangione "apparently hated the medical community because of how it treated his sick relative." In the manifesto, Mangione claims to have acted alone. He has since been arrested and charged with murder and firearms violations.

Daniel Penny Is Acquitted in Death of Jordan Neely on Subway

New York Times, 12/10/2024

Daniel Penny, a former Marine who choked a fellow subway rider on an uptown F train last year, was acquitted on a charge of criminally negligent homicide on Monday, ending a case that had come to exemplify New York City's post-pandemic struggles. The jurors decided that Mr. Penny's actions were not criminal when he held the rider, Jordan Neely, in a chokehold as the two men struggled on the floor of a subway car on May 1, 2023. Mr. Neely, who was homeless and had a history of mental illness, had strode through the subway car that afternoon, yelling at passengers and frightening them, according to witnesses. <https://www.nytimes.com/2024/12/09/nyregion/daniel-penny-not-guilty-jordan-neely.html>

ANALYST COMMENTARY: On 1 May 2023, Daniel Penny, a 24-year-old white Marine Corps veteran, subdued Jordan Neely, a 30-year-old black mentally ill homeless man, on a New York City subway train with a chokehold after Neely displayed erratic and hostile behavior towards other passengers on the train. After witnessing Neely throw garbage at other passengers, lunge at them, and say "I don't have food, I don't have a drink, I'm fed up. I don't mind going to jail and getting life in prison. I'm ready to die ... I will kill," Penny approached Neely behind and placed him into a chokehold. Two other passengers also assisted in subduing Neely by holding his legs while Penny held the chokehold. Penny held the chokehold on Neely for approximately five minutes, and Neely later died in the hospital, the cause of which remains debated. The incident garnered a significant public following and became a political talking point, and in the following weeks Penny was charged with criminally negligent homicide in addition to second-degree manslaughter. On 6 December 2024, the manslaughter charge was dismissed, and on 9 December 2024, Penny was found not guilty of criminally negligent homicide. Throughout the trial, protestors and counter-protestors were both present outside the courthouse, and on the morning of the decision the two sides clashed and needed to be separated by police.

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,
& SURFACE TRANSPORTATION



Following the decision, Walter ‘Hawk’ Newsome, a co-founder of Black Lives Matter (BLM) Greater New York, appeared to threaten Penny, claiming that “it’s a small world, buddy,” and gave a speech denouncing the outcome of the trial and advocating for vigilante activity against perceived oppressors. According to media outlets, Newsome said, “Everybody else has vigilantes. We need some black vigilantes ... People want to jump up and choke us and kill us for being loud, how about we do the same when they attempt to oppress us.” The case has also resulted in an increased focus on mental health issues, with mental health advocates claiming the case illustrates “systemic failures in crisis response.” In particular, they point out that had Neely, who may have been experiencing a mental health episode at the time of the incident, encountered professionals trained in de-escalation rather than civilians, the incident may have unfolded differently. De-escalation techniques can be found in the Cybersecurity and Infrastructure Security Agency’s (CISA) De-escalation Action Guide at : https://www.cisa.gov/sites/default/files/2024-12/CISA_De-escalation-Action-Guide_v508_20241202.pdf

DoD Announces Strategy for Countering Unmanned Systems

Department of Defense, 12/5/2024

On December 2 Secretary of Defense Lloyd J. Austin III signed a classified Strategy for Countering Unmanned Systems. The strategy unifies the Department’s approach to countering these systems that looks across domains, characteristics, and timeframes. Unmanned systems pose both an urgent and enduring threat to U.S. personnel, facilities, and assets overseas. Unmanned aerial systems, most commonly known as drones, pose the most significant threat at this time and increasingly in the US homeland. These threats are changing how wars are fought. By producing a singular Strategy for Countering Unmanned Systems, the Secretary and the Department are orienting around a common understanding of the challenge and a shared approach to addressing it. The strategy builds on other major DoD initiatives, including the standup of the Joint Counter-Small UAS Office, the establishment of a Warfighter Senior Integration Group to meet urgent operational needs, and the launch of the Replicator 2 initiative to defend against the threats of small aerial systems at our most critical installations and force concentrations.

<https://www.defense.gov/News/Releases/Release/Article/3986597/dod-announces-strategy-for-countering-unmanned-systems/>

Torontonians Will Likely Spend One Year And Seven Months Of Their Life On Public Transit: Report CP24, 12/10/2024

Torontonians who commute to work everyday will likely spend about one year and seven months of their life on public transit, according to a new report. Moovit, a public transit app, reached this finding by aggregating data from millions of trips conducted through their platform from 50 cities across the globe. It used metrics like commute and wait times, the number of transfers, public transit improvement factors and payment preferences to illustrate the average experience for commuters. According to 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,
& SURFACE TRANSPORTATION



2024 Global Public Transport Report, the average commute time in Toronto – travelling one way – is about 55 minutes, which is about five minutes behind Vancouver, the longest in the continent. Miami has the third longest commute times in North America at 52 minutes, the report found. Moovit calculated how long commuters spend on public transit over the course of their lifetime by doubling the average one-way commute duration before multiplying by 250, the number of weekdays in a year, over 30 a year period, to account for the number of years a person will work.

<https://www.cp24.com/local/toronto/2024/12/10/torontonians-will-likely-spend-one-year-and-seven-months-of-their-life-on-public-transit-report/>

Public Safety Officials Gather In Minneapolis For National Conference

MPR News, 12/10/2024

At a public safety conference in Minneapolis this week, law enforcement officials from across the country are marking progress in addressing violent crime. The conference for participants in Department of Justice safety programs opened Monday, with Minneapolis officials welcoming hundreds of participants to the city. Minneapolis Police Chief Brian O'Hara took stock of this year's crime statistics in the city. He said violent crime is still trending down from a spike in 2020-21 — but the homicide rate is up from last year. O'Hara said the department has so far logged one more homicide in 2024, than the total for all of 2023. "We've obviously had a number of challenges this year. There are places in the city that have been spiking and have experienced more violence than they have in the past," O'Hara said. He said the increase in homicides is driven by increased violence on the city's south side.

<https://www.mprnews.org/story/2024/12/10/public-safety-officials-gather-in-minneapolis-for-national-conference>

Disabled BART Train In Oakland Causes Major Delays

NBC, 12/9/2024

[Oakland, California] A disabled train on the tracks in Oakland caused major delays Monday morning on BART. The train was stalled between the Coliseum and Fruitvale stations and BART crews are bringing another train alongside it to transfer passengers and bring them to the nearest station, BART spokesperson Jim Allison said. The disabled train broke down about 7 a.m. The incident is causing major delays on the Berryessa Line in all directions. There is limited Green line service between Berryessa and Daly City, BART officials said. Passengers traveling from the San Francisco line can board a Dublin/Pleasanton train and transfer at Bayfair to a Berryessa train. Those traveling from the Berryessa line can board a Richmond train and transfer at Bayfair to a Daly City train.

<https://www.nbcbayarea.com/news/local/east-bay/disabled-bart-train-oakland/3731282/>

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,
& SURFACE TRANSPORTATION



CYBERSECURITY

Cisco Warns of Attacks Exploiting Decade-Old ASA Vulnerability *Security Week, 12/3/2024*

Cisco on Monday updated an advisory covering a decade-old vulnerability to warn customers about in-the-wild exploitation. The vulnerability is tracked as CVE-2014-2120 and it has been described as a medium-severity cross-site scripting (XSS) vulnerability affecting the WebVPN login page of Cisco Adaptive Security Appliance (ASA) products. According to the networking giant, an unauthenticated, remote attacker can exploit the vulnerability to conduct XSS attacks against WebVPN users by getting them to click on a malicious link. Cisco published its initial advisory for CVE-2014-2120 in March 2014, when it informed customers that they should reach out to support channels to obtain a patched software version. "In November 2024, the Cisco Product Security Incident Response Team (PSIRT) became aware of additional attempted exploitation of this vulnerability in the wild. Cisco continues to strongly recommend that customers upgrade to a fixed software release to remediate this vulnerability," Cisco said in an update added on December 2. <https://www.securityweek.com/cisco-warns-of-attacks-exploiting-decade-old-asa-vulnerability/>

ANALYST COMMENTARY: CVE-2014-2120, a medium-severity cross-site scripting (XSS) vulnerability in the WebVPN login page of Cisco ASA products, has seen renewed exploitation nearly a decade after its disclosure. Originally patched in 2014, the vulnerability allows unauthenticated attackers to execute XSS attacks by luring victims into clicking malicious links. While Cisco urged customers to update to a patched release in 2014, its inclusion in CISA's Known Exploited Vulnerabilities catalog and recent exploitation by the AndroXgh0st botnet highlight the persistent risk of unpatched systems. AndroXgh0st, linked to compromises of hundreds of devices, has adapted its techniques to include CVE-2014-2120 among numerous vulnerabilities exploited across a broad range of technologies, such as Cisco, Atlassian, and WordPress plugins. Notably, the botnet is leveraging the vulnerability to upload arbitrary files and backdoor servers via malicious PHP code, enabling long-term persistence and control. This tactic positions compromised devices for subsequent activities like credential theft, cryptocurrency mining, and DDoS attacks. The renewed focus on CVE-2014-2120 emphasizes the critical importance of applying security updates promptly, even for older vulnerabilities. Organizations using Cisco ASA or similar products should immediately verify their software versions and upgrade if necessary. The broader integration of AndroXgh0st with vulnerabilities across diverse systems also stresses the need for comprehensive security practices, including regular patching, monitoring for unusual activity, and securing VPN endpoints to mitigate potential exploits and reduce exposure to such botnet campaigns.

NOT FOR PUBLIC DISSEMINATION

*** FAIR USE NOTICE ***

This message contains copyrighted material whose use has not been specifically authorized by the copyright owner. The PT 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 PT ISAC: 866.784.7221 or email st-isac@surface transportationisac.org