Information Sharing & Analysis Center

PUBLIC TRANSPORTATION & OVER THE ROAD BUS

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

February 4, 2025

## SUSPICIOUS ACTIVITY & INCIDENT REPORTS

**Body Found On Subway In Times Square**
*NBC, 2/3/2025*

[New York] Authorities are investigating the death of a man whose body was found on a No. 1 train in Times Square Sunday, according to police. The NYPD says the man is thought to be between the ages of 60 and 70. He has not been identified. No criminality is suspected at this time. Delays were reported in the area as authorities investigated. The probe is ongoing.
https://www.nbcnewyork.com/manhattan/subway-delay-body-times-square/6132895/

**Man Wounded After Argument Leads To Stabbing On CTA Red Line Train, Police Say**
*CBS, 2/1/2025*

[Chicago, Illinois A 44-year-old man was hospitalized Saturday morning after he was stabbed during a fight on a CTA Red Line Train. The incident happened in the 1100 block of West Bryn Mawr Avenue in the Edgewater neighborhood just before 6:30 a.m. Chicago police said the victim was arguing with another unknown man on the train that turned into a fight. During this, the offender pulled out a sharp object and swung it at the victim. The victim suffered cuts to the abdomen and hand. He was taken to St. Francis Hospital in fair condition. As of Saturday, there is no one in custody.
https://www.cbsnews.com/chicago/news/man-wounded-stabbing-cta-red-line-train/

**CATS Bus Rider Tells Charlotte Police A Man He Didn't Know Fired A Gun To Intimidate Him**
*Charlotte Observer, 2/3/2025*

[Charlotte, North Carolina] A 32-year-old man alleged another person pointed a gun at him and then fired on a bus in east Charlotte to be intimidating Thursday night, according to a Charlotte-Mecklenburg police report. He was uninjured. The shooting occurred inside of a Charlotte Area Transit System bus at 10:29 p.m. near 6810 Lawyers Road, the police report said, by an "unknown suspect." The police report said the victim didn't know the shooter. The CMPD public affairs division declined to answer questions about the case. CATS has not offered any comment.
https://www.charlotteobserver.com/news/local/crime/article299637994.html

## TERRORISM & EXTREMISM

**Australia Follows US, Britain In Sanctioning 'Terrorgram' Extremist Network**
*SCMP, 2/3/2025*

[Australia] Australia on Monday imposed sanctions on extreme right-wing online network "Terrorgram" as part of its efforts to combat a rise in antisemitism and online extremism, following similar moves by Britain and the United States. Foreign Minister Penny Wong said the government's action would make it a criminal offence to engage with "Terrorgram" and help prevent children from becoming caught up in far-right extremism. "Terrorgram is an online network that promotes white supremacy and racially-motivated violence," Wong said in a statement. "It is the first time any Australian government has imposed counterterrorism financing sanctions on an entity based entirely online." Offenders will face up to 10 years in jail and heavy fines, she said. The Australian government also renewed sanctions on four right-wing groups: the National Socialist Order, the Russian Imperial Movement, Sonnenkrieg Division and The Base, Wong said. https://www.scmp.com/news/asia/australasia/article/3297157/australia-follows-us-britain-sanctioning-terrorgram-extremist-network

**Man Admits Setting Fire To Koran During Livestream Near Terror Attack Memorial**
*Metro, 2/3/2025*

[United Kingdom] A man has admitted setting a copy of Islam's holy book alight and livestreaming it on social media. Martin Frost ripped pages out of the Koran near the Glade of Light memorial to the 22 victims of the 2017 Manchester Arena bombing, before setting them on fire. He publicized it beforehand and streamed it on social media on Saturday, setting the pages alight before dropping them to the ground and stomping on them. Metro has chosen not to share footage of the book being burned, which is seen as a blasphemous act by Muslims as they consider the Koran to be the literal word of God. Frost, 47, was arrested shortly afterwards. He appeared at Manchester magistrates court today where he admitted a racially aggravated public order offence. The court was told the 'trigger' for his actions was the death of his daughter in the Israeli conflict. He was also filmed holding an Israel flag before setting pages of the Koran alight. https://metro.co.uk/2025/02/03/man-admits-setting-fire-to-koran-during-livestream-near-terror-attack-memorial-22489203/

**Birmingham Man Guilty Of Planning A Terrorism Attack**
*Counterterrorism Police, 1/30/2025*

[United Kingdom] A Birmingham man has today been found guilty of planning an attack against a mosque and a bookshop in the city. Jason Savage, aged 35 from Fourth Avenue, Small Heath, was convicted following a trial at Birmingham Crown Court. The jury heard how Savage – since March 2022 and up until his arrest in March 2024 – had researched and planned activity to carry out an attack.

Savage had converted to Islam in the 2010s and followed an extreme and violent interpretation of the Salafi movement. Prosecutors told the court that Savage had targeted a Salafi cleric associated with a mosque and bookstore in Small Heath because the cleric was an outspoken critic of Islamist terrorism and extremism contrary to Savage's views. The jury were shown what was described as a reconnaissance video which was made by Savage three days before his arrest. It shows him walking round the location of the mosque and bookstore, discussing points of entry, the routes that the police would likely attend from and escape routes. Savage also downloaded and watched violent and extremist videos, researched how to kill with a knife and how to make parts of a gun and ammunition as well as carrying out the reconnaissance of military buildings and police stations as potential locations.
https://www.counterterrorism.police.uk/birmingham-man-guilty-of-planning-a-terrorism-attack/

## SECURITY & SAFETY AWARENESS

**Fare Evasion Down On MTA Systems During Past Six Months**
*Mass Transit Magazine, 2/3/2025*

[New York] The Metropolitan Transportation Authority (MTA) has seen a decrease in fare evasion during the past six months. According to the agency, from June 2024 through December 2024, subway fare evasion went down 26 percent. Across buses, including both the local and express bus network, fare evasion went down by 9.1 percent over the same period of time. MTA says the progress in fare evasion follows a comprehensive strategic response implemented by New York Gov. Kathy Hochul, the New York Police Department (NYPD) and MTA — including strategic deployment of enforcement, modifications to fare gates at numerous transit stations and other measures helping to reduce fare evasion. The authority is installing new anti-fare evasion measures at all subway turnstiles this year and new fare gates are being installed at 20 high-traffic stations this year. https://www.masstransitmag.com/technology/fare-collection/press-release/55265174/mta-new-york-city-transit-fare-evasion-down-on-mta-systems-during-past-six-months

**ANALYST COMMENTARY: Fare evasion is a commonly cited item of interest for major transit organizations nationwide, with larger agencies reporting significant losses to fare evasion each year. The Metropolitan Transportation Authority (MTA) reported that they lost $690 million to fare evasion in 2022, and the Washington Metropolitan Area Transit Authority (WMATA) has claimed that approximately 70 percent of bus riders were not paying their fares in 2024, up from the 17 percent who did not pay fares in pre pandemic years. Multiple transit agencies have noted a link between violent offenders and fare evasion. MTA CEO Janno Lieber has remarked that while "not every fare evader is a criminal," virtually all criminals "evaded the fare." Los Angeles Metro officials have echoed this sentiment, and a study of violent crime related arrests on the Los Angeles transit system from May 2023 to April 2024 found that 94 percent of people arrested for violent crimes on the Los Angeles**

**transit system had not paid their fare. To combat fare evasion, in May 2024 the Los Angeles Metro piloted a Tap to Exit program at their North Hollywood Station that requires riders to tap their Metro card upon arriving at the destination to ensure their trip was paid for. Those who were caught evading the fare were removed from the system and, in some cases, cited. By September 2024, 91 percent of riders at the North Hollywood Station reported the pilot program "made the station feel cleaner" and 86 percent claimed it "made them feel safer." Transit officials also claimed the Tap to Exit program resulted in a 40 percent decrease in reported crime.**

**Crime On Metro Transit Fell Last Year As Agency Cracks Down On Smoking**
*Star Tribune, 2/3/2025*

[Minnesota] Metro Transit's resurgence continued last year as ridership on buses and trains rose for the third consecutive year, while reported crime, one of the factors that has kept riders away, fell by 6%, agency officials said Monday. The state's largest transit agency provided 47.5 million rides from January through December, which marked a nearly 6% increase over the previous year. That was still far below the 85.8 million in 2015, which was the strongest year of ridership in the past few decades. "We are strengthening our network and providing additional quality transit service across our region," General Manager Lesley Kandaras said. Two factors helped fuel Metro Transit's year-over-year growth. The agency combatted an ongoing operator shortage. With 450 additional bus and train operators compared to last year, Metro Transit increased frequency on light-rail trains and some bus routes while bringing scuttled routes back. https://www.startribune.com/crime-on-metro-transit-fell-last-year-as-agency-cracks-down-on-smoking/601216247

**RTD Introduces A New Detective Force To Improve Users' Safety**
*Denver Post, 2/1/2025*

[Colorado] The Regional Transportation District police department has introduced a new detective force to investigate criminal activity across the district. This new force, a response to riders' safety concerns, is expected to be fully operational by the end of 2025. Officials said the department is part of RTD's effort to increase safety on its property. Riders and operators reported thousands of assaults on drivers, public urination and rampant drug use between 2021 and 2024. Officials said the new department should make it easier to investigate crimes across the district, which encompasses parts of eight metro counties. Brian Cousineau, the commander of the new detective force, pointed to copper wire theft as an example of how it could investigate crimes differently in an RTD press release. Instead of investigating individual cases with local law enforcement agencies, RTD detectives can investigate multiple instances of similar crimes across counties as a single case. The commander explained that this could lead to such crimes being prosecuted as felonies, instead of individual misdemeanors. https://www.denverpost.com/2025/02/01/rtd-new-detective-force-safety/

**Bill Requiring Amtrak Refunds For Cancelled, Late Trains Is Introduced**
*Trains, 2/3/2025*

A New Jersey congressmen has introduced a bill first announced last summer that would require Amtrak to provide passengers with ticket refunds when trains are cancelled or delayed "due to a failure of Amtrak." H.R. 769 was introduced by U.S. Rep. Josh Gottheimer (D-N.J.) on Jan. 28 and sent to the House Committee on Transportation and Infrastructure. Rep. Thomas Kean (R-N.J.) is cosponsor. Gottheimer had announced the bill last August [see "Congressman wants Amtrak …," Trains News Wire, Aug. 13, 2024] but it was not introduced during the 2023-24 term. "It can take time to draft and negotiate the technical details," Gottheimer spokesman Tony Wen told NJ.com, "but the ultimate outcome will be worth it." Text of the bill is not yet available on the Congress website. https://www.trains.com/trn/news-reviews/news-wire/bill-requiring-amtrak-refunds-for-cancelled-late-trains-is-introduced/

## CYBERSECURITY

**Italy's Regulator Blocks Chinese AI App DeepSeek On Data Protection**
*Reuters, 2/4/2025*

Italy's data protection authority, the Garante, said on Thursday it had ordered DeepSeek to block its chatbot in the country after the Chinese artificial intelligence startup failed to address the regulator's concerns over its privacy policy. The watchdog had questioned DeepSeek this week about its use of personal data, particularly seeking information on what personal data is collected, from which sources, for what purposes, on what legal basis and whether it is stored in China. The Garante's order - aimed at protecting Italian users' data - came after the Chinese companies that supply the DeepSeek chatbot service provided information that "was considered to totally insufficient," the watchdog said in a statement. DeepSeek had no immediate comment. The Chinese startup said its newly-launched AI models are on a par or better than industry-leading models in the United States at a fraction of the cost, threatening to upset the technology world order.. https://www.reuters.com/technology/artificial-intelligence/italys-privacy-watchdog-blocks-chinese-ai-app-deepseek-2025-01-30/

**ANALYST COMMENTARY: In 2015, the People's Republic of China (PRC) launched their "Made in China 2025" plan, which "identified the control of data as a key to [China's] ambitions." The same year, the PRC announced the Digital Silk Road (DSR) component of their existing Belt and Road Initiative, which was heavily promoted the development of digital technology in China to reduce the PRC's reliance on Western digital technology and was intended to result in the global adoption of digital technology owned by Chinese entities. In addition to prompting significant growth in the Chinese private sector, the DSR has also served as a tremendous intelligence collection campaign for the PRC as Chinese companies are legally required to keep the data collected by exported Chinese technology available to**

**the PRC for the express purpose that the information can be exploited by analysts. In 2017, China's National Intelligence Law compelled Chinese software manufacturers to install backdoors in their software and devices, offering incentives for those who complied, and penalizing those who refused. In 2021, the Cyberspace Administration of China (CAC), which is responsible for regulating and censoring information available on the Internet in the People's Republic of China (PRC), enacted a series of regulations regarding the disclosure of software vulnerabilities found in Chinese-made software. Among these regulations, the CAC mandated that Chinese companies "must share all vulnerability reports with the Ministry of Industry and Information Technology (MIIT) within two days" while simultaneously making it illegal for individuals and organizations to "collect, sell, or publish information on network product security vulnerabilities." These regulations have concerned cybersecurity experts on a global scale, as they allow the PRC to aggregate (and exploit) existing software vulnerabilities – including those identified by the manufacturers of the software - before the vulnerabilities are patched or even shared with the international community. This has led to many Western nations banning and warning against the use and ownership of Chinese-owned or manufactured devices and software that collects data due to fears that the data is relayed back to China and exploited for intelligence purposes. In particular, experts have warned against the use of software and devices that collect sensory information, like social media applications, cameras, GPS devices, video editing software, and chatbots. Consumers often overlook the overt risks and intelligence collecting capabilities of Chinese-manufactured software and devices because the software and devices are often significantly cheaper than their non-Chinese made counterparts or have a widespread following that can give off the false illusion that they are safe and secure.**

**New TorNet Backdoor Seen In Widespread Campaign**
*CISCO Talus, 1/28/2025*

Cisco Talos discovered an ongoing malicious campaign operated by a financially motivated threat actor since as early as July 2024 targeting users, predominantly in Poland and Germany, based on the phishing email language. The actor has delivered different payloads, including Agent Tesla, Snake Keylogger, and a new undocumented backdoor we are calling TorNet, dropped by PureCrypter malware. The actor is running a Windows scheduled task on victim machines—including on endpoints with a low battery—to achieve persistence. The actor also disconnects the victim machine from the network before dropping the payload and then connects it back to the network, allowing them to evade detection by cloud antimalware solutions. We also found that the actor connects the victim's machine to the TOR network using the TorNet backdoor for stealthy command and control (C2) communications and detection evasion. https://blog.talosintelligence.com/new-tornet-backdoor-campaign/

**ANALYST COMMENTARY: This campaign reflects a growing trend where financially motivated threat actors leverage multi-stage malware delivery chains and increasingly sophisticated evasion tactics to bypass both endpoint and cloud-based defenses. The use of PureCrypter to deploy an undocumented**

**backdoor like TorNet, coupled with anti-debugging, anti-VM, and anti-sandbox techniques, signals a higher level of operational security awareness. Disconnecting victims from the network before payload deployment is a particularly clever move, sidestepping cloud antivirus solutions that rely on real-time telemetry. The fact that persistence mechanisms remain active even on low battery power shows the actor's intent to maintain control for as long as possible, a tactic that suggests they anticipate lengthy dwell times for financial exploitation. The incorporation of Tor for anonymized C2 communications complicates detection and response, as traditional network monitoring tools may miss or misclassify traffic routed through the TOR network. This also poses challenges for threat hunters relying on typical indicators like known IPs or domains. While Cisco offers robust protections within its ecosystem, organizations should also consider broader defensive strategies, including tightening email gateway controls against compressed archives like .tgz, monitoring for unusual network reconfigurations (such as DHCP lease changes), and leveraging endpoint detection solutions capable of identifying reflective DLL injection and unauthorized process persistence. A proactive approach, such as threat hunting for anomalous use of scheduled tasks or the appearance of TOR-related processes on endpoints, could help mitigate risks before significant financial damage occurs.**