Information Sharing & Analysis Center

PUBLIC TRANSPORTATION & OVER THE ROAD BUS

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

February 5, 2025

## SUSPICIOUS ACTIVITY & INCIDENT REPORTS

**Belgian Police Hunt For Armed Gunmen After Shooting In Brussels**
*NBC, 2/5/2025*

[Brussels, Belgium] A manhunt has been launched for two suspected gunmen who fled into the subway tunnels of the Belgian capital of Brussels after a shooting on Wednesday, the Brussels Prosecutor's office said in a statement to NBC News. Police were called to a shooting above the Clemenceau subway station in central Brussels around 6 a.m. local time (12:00 a.m. ET), the office said. A major search operation was carried out after video-surveillance footage showed the two suspects, with police finding several shell casings on site. … The prosecutor's office said no one was injured. It added that no one had been arrested so far, but that the investigation was ongoing. There was no indication of a terrorist motive, it said. https://www.nbcnews.com/news/world/belgian-police-hunt-armed-gunmen-shooting-brussels-rcna190756

**ANALYST COMMENTARY: On 4 February 2025 at approximately 6:00 p.m. Belgium time, two men armed with AK-pattern carbines opened fire in the Clemenceau metro station in central Brussels, Belgium. It is unclear what the men were shooting at, and no injuries have been reported. The incident was caught on CCTV, the video from which shows the men firing their weapons for a few seconds, then fleeing down into the subway with their weapons. The section of the station they fired their weapons in appears to have been sparsely populated at the time of the shooting, and the cameras do not show any crowds present. Neither the men nor their weapons have been located despite an ongoing investigation. Local authorities have said they do not believe that the incident is terrorism related, and media outlets have reported that sources claim the incident stemmed from a drug dispute. A massive police response was launched in response to the incident, and law enforcement closed down three surrounding subway stations for over 18 hours while they investigated the scene of the shooting and searched nearby subway tunnels for the perpetrators. According to the Flemish Peace Institute, Belgium has the fourth highest rate of gun violence in Europe and has about 20 gun homicides and 4,000 armed robberies reported each year, the numbers of which have declined since the early 2000s.**

**Trains Damaged By 'Projectiles' Thrown At Them**
*BBC, 2/3/2025*

[United Kingdom] Trains have been damaged after being struck by "projectiles" thrown at them, according to police. The incidents were reported between Cambridge and Cambridge North stations at about 17:40 GMT on Sunday. Govia Thameslink Railway said disruption to its services between the city and King's Lynn, in Norfolk, continued throughout Monday. Officers from British Transport Police searched the area but did not identify any suspects. The force said its inquiries were ongoing. https://www.bbc.com/news/articles/cr53le6g7jqo

**Parolee Stabs Man On Midtown Manhattan Subway After Accidental Bump**
*New York Daily News, 2/4/2025*

[New York] A parolee stabbed a man aboard a Midtown Manhattan subway Tuesday after the victim accidentally bumped into him, police sources said. The victim, a man in his 20s, was on a downtown-bound M train heading toward Rockefeller Center just after 2 p.m. when he accidentally bumped into the 23-year-old attacker, sources said. The unhinged man became irate over the bump and punched the victim in the face before pulling out a knife and stabbing him in the right torso. Police responded to the 47th-50th Sts.-Rockefeller Center subway station, where they found the wounded victim. Medics rushed him to Bellevue Hospital, where he was in stable condition. Police arrested the accused stabber, identifying him as Bronx resident Shemar Shaw, and charged him with assault and criminal possession of a weapon. According to police sources, Shaw served more than five years in prison for robbery and assault in a Brooklyn incident and was released on parole in August, plus has additional prior arrests for assault, robbery and criminal mischief. https://www.nydailynews.com/2025/02/04/parolee-stabs-man-midtown-manhattan-train-accidental-bump/

**Man Arrested After Barricading Himself In TriMet Bus After Firing Shots, Police Say**
*KOIN, 1/29/2025*

[Portland, Oregon] Portland police arrested a man on Wednesday after he allegedly barricaded himself inside a TriMet bus. Police identified the suspect as 33-year-old Portland resident Hosea J. Chambers. He was booked into the Multnomah County Detention Center and is accused of several crimes, including kidnapping and robbery. The standoff ended after the Portland Police Bureau said officers were on the scene negotiating with a suspect after he allegedly fired shots and then boarded a TriMet bus downtown. Authorities said dozens of officers responded to the incident near Northwest 5th Avenue and Northwest Glisan Street as police tried for multiple hours to convince someone inside a bus to leave. According to police, the bus driver helped get all the passengers off the bus as the armed suspect boarded. “While officers managed to recover the firearm, the suspect remained on the bus and refused

to exit," the Portland Police Bureau said in a press release. https://www.koin.com/news/portland/man-barricading-himself-in-trimet-bus-01292025/

**Metro Train Collides with Car in Historic South-Central**
*My News LA, 2/3/2025*

[Los Angeles, California] A Metro Blue (A) Line train collided with a vehicle in the Historic South-Central neighborhood Monday, but no injuries were reported. The train running between Grant/LATTC and San Pedro Street stations hit the vehicle near East Washington Boulevard and Los Angeles Street around noon Monday, according to the Los Angeles Fire Department. Train service continued to the next station, allowing passengers to disembark, the LAFD said. Metro spokesman Dave Sotero said the A line service was affected for at least an hour. "Regular train service has now resumed throughout the line," Sotero said in a statement. "Metro reminds all drivers to be rail safe, pay attention to traffic signals, and always look both ways." Both the vehicle's driver and train passengers were medically assessed at the scene. It was not immediately clear if the train sustained any damage. The collision was under an investigation by the Los Angeles Police Department, Sotero said. https://mynewsla.com/crime/2025/02/03/metro-train-collides-with-vehicle-in-historic-south-central-2/

## TERRORISM & EXTREMISM

**The New Orleans Attack: The Technology Behind IS-Inspired Plots**
*Global Network on Extremism & Technology, 1/30/2025*

The use of technology by terrorists and violent extremists is a perennially trendy issue in counterterrorism (CT) research—and for good reason. Identifying, monitoring, and assessing technological advancements and understanding how these innovations can be or have already been leveraged for malicious purposes is a key component to effectively disrupting terrorist plots. Attempting to stay and remain ahead of emerging technologies and the novel ways in which they might be employed has become an essential component in redressing the "failure of imagination" that led to the 9/11 attacks that saw US domestic commercial flights transformed into lethal weapons by a foreign terrorist organization. Islamic State (IS) and supporters inspired by the group have strategically used technology across a wide spectrum, often combining low- to high-tech tools for a variety of purposes, including recruitment, radicalization, fundraising, financial transactions, attacks, logistical operations, and operational security. The New Orleans IS-inspired New Year's Day attack, which tragically killed 14 people and injured dozens more, has shown again that attackers use tools across the technological spectrum, often in combination, to maximize lethality and minimize detection of the plot before execution, while also reflecting the conditions in which they operate. https://gnet-research.org/2025/01/30/the-new-orleans-attack-the-technology-behind-is-inspired-plots/

# Information Sharing & Analysis Center

PUBLIC TRANSPORTATION
& OVER THE ROAD BUS

## SECURITY & SAFETY AWARENESS

**2 Teenagers Arrested After Queens Subway Joyride, NYPD Says**
*CBS, 2/3/2025*

[New York] Two teenagers have been charged with stealing a New York City subway train and taking it for a joyride, police say. Investigators spent more than a week trying to track down suspects after the R train was reported stolen from a station in Queens on Jan. 25. The suspects charged are 15 and 17 years old, the NYPD said. The younger boy was arrested at his school in Brooklyn, while the older boy was taken into custody at his home. Police said Monday they were looking for four additional suspects. MTA employees told police that people boarded the unoccupied train at 71st Avenue, where out-of-service trains are stored, then drove it a short distance and broke numerous windows in one of the cars. Authorities found a video on social media allegedly showing the subway joyride in action. The footage shows one person operating the controls in the conductor's cabin, a second dangling his legs over the tracks, and a third standing behind him. Surveillance video later released by police shows at least six people inside the train car. https://www.cbsnews.com/newyork/news/subway-joyride-2-teens-charged-nypd-says/

**Hey San Francisco, Speed Safety Cameras are Coming**
*SFMTA, 1/27/2025*

[San Francisco, California] This week, you may start seeing ads throughout San Francisco about the city's new speed safety camera program. A public information campaign is kicking off to share the news that speed cameras will begin operating in March 2025. The campaign advises drivers to: Travel at a safe speed, Remember their role in keeping people safe on the road. The educational program will include ads on billboards and bus shelters as well as web and social media ads. This will help people adjust to a new form of speed enforcement that's coming to San Francisco. Starting in March, speed safety cameras will begin operating at up to 33 locations across the city. The speed safety cameras will be placed on streets where speeding vehicles are a known issue. … The speed safety cameras will photograph the rear license plate of vehicles traveling 11 MPH or more over the posted speed limit. Next, the registered owner of the vehicle will receive a citation. Fee amounts are set by the state and vary based on the speed violation. https://www.sfmta.com/blog/hey-san-francisco-speed-safety-cameras-are-coming

**King County Metro Unveils Latest Idea For Keeping Bus Drivers Safer**
*Seattle Times, 2/4/2025*

[Seattle, Washington] If you ride King County Metro buses, you've seen them: the clear plastic gates known as "sneeze guards," that swing between the driver and the front door. They were meant to protect drivers during the COVID-19 pandemic, but aren't strong enough to thwart an attacker, and with

assaults on Metro drivers a continuing problem, the agency and the drivers' union are looking to install heavier partitions that lock. Plans have been discussed for months but gained political urgency since the fatal stabbing of a bus driver in December. Drivers could open the new gates when needed, for instance to leave their seat to strap a customer's wheelchair in place, or reset a dislodged trolleybus pole to the outdoor power wires. "If nothing else, it brings some operators some peace of mind," said Greg Woodfill, Amalgamated Transit Union Local 587 president. "Some of them are terrified to go to work. … It's not the total solution, but it's a start." The county's rough estimate is $15.1 million for 1,200 buses. https://www.seattletimes.com/seattle-news/transportation/king-county-metro-unveils-latest-idea-for-keeping-bus-drivers-safer/

## CYBERSECURITY

**Researchers Link DeepSeek's Blockbuster Chatbot To Chinese Telecom Banned From Doing Business In US**

*Reuters, 2/5/2025*

The website of the Chinese artificial intelligence company DeepSeek, whose chatbot became the most downloaded app in the United States, has computer code that could send some user login information to a Chinese state-owned telecommunications company that has been barred from operating in the United States, security researchers say. The web login page of DeepSeek's chatbot contains heavily obfuscated computer script that when deciphered shows connections to computer infrastructure owned by China Mobile, a state-owned telecommunications company. The code appears to be part of the account creation and user login process for DeepSeek. In its privacy policy, DeepSeek acknowledged storing data on servers inside the People's Republic of China. But its chatbot appears more directly tied to the Chinese state than previously known through the link revealed by researchers to China Mobile. The U.S. has claimed there are close ties between China Mobile and the Chinese military as justification for placing limited sanctions on the company. https://apnews.com/article/deepseek-china-generative-ai-internet-security-concerns-c52562f8c4760a81c4f76bc5fbdebad0

**ANALYST COMMENTARY: In recent years, the People's Republic of China (PRC) has launched several initiatives that pursue Chinese political, social, economic, technological, and military development, with the ultimate goal of significantly increasing China's national power by 2049. According to the Department of State, as part of one of these initiatives known as Military-Civil Fusion (MCF), the PRC has been eliminating barriers between "China's civilian research and commercial sectors and its military and defense industrial sectors" to advance their military capabilities and ensure that all Chinese innovation serves both economic and military purposes. In doing this, Chinese software and technology providers are increasingly providing data collected abroad to the PRC for further exploitation, which furthers Chinese intelligence collection goals. In some instances, this provides the**

**PRC with sensitive proprietary information stolen from Western industries which are then used to augment China's military and industrial capabilities. To protect U.S. individuals, organizations, and interests from exploitation by the PRC, and to limit the amount of technology that China steals from the U.S., the U.S. government has been publishing the names of Chinese companies believed to be involved in furthering the PRC's MCF goal (and, in some cases, sanctioning them) in hopes that American people and organizations will begin to view the companies as PRC military suppliers rather than as innocuous routine commercial entities. These efforts have had limited success, and despite the overt national security concerns posed by and risks associated with using Chinese technology and software, Americans continue to download and use it, which creates vulnerabilities. In a recent example, on 20 January 2025 Chinese artificial intelligence platform DeepSeek released its first free AI chatbot, akin to ChatGPT. By 27 January 2025, DeepSeek became the most downloaded app in the U.S. app store for iOS. Within days, Canadian cybersecurity firm Feroot Security reported that code on the DeepSeek platform contained "hidden capabilities enabling direct data transmission from DeepSeek to China Mobile servers." While unsurprising, this is significant because China Mobile was sanctioned by a U.S. Executive Order in 2020 due to its strong MCF ties to the People's Liberation Army, and its subsidiaries were also listed as national security threats by the Federal Communications Commission in 2022. In other words, search queries, data entries, and data generation entered into and conducted by DeepSeek (which is the most downloaded free app for U.S. iOS devices) is available to China Mobile or exploitation, which has been sanctioned due to national security concerns stemming from its strong ties to adversarial military forces.**

**Aquabot Botnet Targeting Vulnerable Mitel Phones**
*Security Week, 1/29/2025*

A Mirai-based malware family this month started targeting vulnerable Mitel SIP phones to ensnare them into a botnet capable of distributed denial-of-service (DDoS) attacks, Akamai reports. The malware, called Aquabot, attempts to exploit CVE-2024-41710, a high-severity command injection vulnerability affecting Mitel 6800, 6900, and 6900w series SIP phones, including 6970 Conference Unit. In July 2024, Mitel announced firmware updates that patch the flaw, warning that its successful exploitation "could allow an authenticated attacker with administrative privilege to conduct a command injection attack due to insufficient parameter sanitization during the boot process". "A successful exploit of this vulnerability could allow an attacker to execute arbitrary commands within the context of the phone, with potential impacts on the confidentiality, integrity, and availability of the device," Mitel said.
https://www.securityweek.com/aquabot-botnet-targeting-vulnerable-mitel-phones/

**ANALYST COMMENTARY: Attackers are once again capitalizing on publicly available proof-of-concept exploits, this time targeting Mitel SIP phones with Aquabot, a Mirai-based botnet malware. CVE-2024-41710 allows attackers to execute arbitrary commands via crafted HTTP POST requests, enabling them to compromise devices and recruit them for DDoS attacks. What's troubling is that Aquabot isn't just**

**focused on Mitel—it's also targeting Hadoop YARN, Roxy-WI, and various routers, showing a broader strategy aimed at IoT and enterprise infrastructure. The fact that exploitation began six months after disclosure reinforces the need for rapid patching, especially in IoT environments where security updates are often delayed. Since SIP phones aren't typically monitored for malware infections, businesses should implement strict firewall rules, segment VoIP networks, and watch for abnormal outbound traffic. Another concern is Aquabot's ability to report back to its command-and-control infrastructure when certain signals are detected, indicating that attackers are refining their ability to maintain long-term control over infected devices. With CISA already warning about other exploited Mitel vulnerabilities, organizations should proactively audit their VoIP and collaboration tools. Botnets like Mirai continue evolving, and without strong security controls, critical communication systems remain an easy target for attackers.**