

# Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,  
OVER THE ROAD BUS,  
& SURFACE TRANSPORTATION



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

December 6, 2024

### SUSPICIOUS ACTIVITY & INCIDENT REPORTS

#### **Woman Stabs Person In Neck With Screwdriver At Bus Station**

*Action 5 News, 12/5/2024*

[Memphis, Tennessee] A woman stabbed a person at the bus station Friday morning. According to Memphis Police, the stabbing happened at Greyhound on Airways Boulevard around 4:30 a.m. A witness told police he saw a woman stabbed a person in the neck with a screwdriver. The victim was taken to Regional One Hospital in critical condition. Police said the victim has an active warrant out of Mississippi, and Mississippi said they do not want to extradite. The suspect is 5'5 and in her mid-20s with a heavy build. <https://www.actionnews5.com/2024/12/06/woman-stabs-person-neck-with-screwdriver-bus-station/>

#### **Possible Drones In New Jersey Spotted Over Critical Infrastructure, Police Chief Says**

*CBS News, 12/5/2024*

[New Jersey] The mystery in the skies over New Jersey continues. One law enforcement official said flying objects, possibly drones, were seen over critical infrastructure, while residents have reported seeing some hovering over their homes in the northern and central parts of the state. The FBI is investigating the clusters of possible drones reported over the last few weeks. The bureau is still asking residents to send in pictures and videos. Anyone with information can call the FBI at 1-800-CALLFBI, or submit online here: <https://tips.fbi.gov/home>. Florham Park's police chief sent a message to residents that says drone sightings have been reported above "water reservoirs, electric transmission lines, rail stations, police departments, and military installations." He added that "their presence appears nefarious in nature." New Jersey Gov. Phil Murphy posted on social media Thursday... "We are actively monitoring the situation and in close coordination with our federal and law enforcement partners on this matter. There is no known threat to the public at this time" ... In Somerset County last week, officials had to cancel an emergency medical helicopter transport because drones were seen near the landing area. <https://www.cbsnews.com/newyork/news/new-jersey-drones-objects-morris-county-somerset-county/>

**ANALYST COMMENTARY: Reports of suspicious Unmanned Aircraft System (UAS) sightings from pilots, citizens, and law enforcement remain high. The Federal Aviation Administration (FAA) receives over 100 such reports each month. The agency encourages the public to report unauthorized drone operations to local law enforcement. UAS or "drones" are prohibited from flying over designated**

#### **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



national security-sensitive facilities. According to the FAA, "Operations are prohibited from the ground up to 400 feet above ground level and apply to all types and purposes of UAS flight operations". Flight restrictions exist over many public venues, landmarks, and other locations, including some critical infrastructure and all active emergency or rescue operations. The FAA's B4UFLY service provides situational awareness to recreational flyers and other drone users, including information on controlled airspace, special use airspace, critical infrastructure, airports, national parks, and military training routes. Additional information is available here: [https://www.faa.gov/uas/getting\\_started/b4ufly](https://www.faa.gov/uas/getting_started/b4ufly).

## **BART, Ferries Recover Quickly After Northern California Earthquake, Tsunami Warning** *CBS News, 12/5/2024*

[San Francisco, California] Thursday's earthquake that struck Northern California and the tsunami warning that followed had led to transportation impacts across the Bay Area, including a shutdown of BART through the Transbay Tube. The earthquake, which had a preliminary magnitude of 7.0, struck at 10:44 p.m. in the ocean west of the community of Petrolia, which prompted a tsunami warning for coastal communities and orders by authorities to move to higher ground. Officials with the U.S. National Tsunami Warning Center announced that the warning has been lifted shortly before noon. Shortly before 11 a.m., BART announced that service was stopped in the tunnel connecting Oakland and San Francisco. Several minutes later, BART announced that there was a "major delay" in all directions and that the tube remained closed. Around noon, the agency announced that normal service has resumed, but delays continued into the afternoon. <https://www.cbsnews.com/sanfrancisco/news/northern-california-earthquake-humboldt-coast-bart-transbay-tube-service-halted/>

**ANALYST COMMENTARY:** At approximately 10:44 a.m. on 5 December 2024, a magnitude 7.0 earthquake struck off the Northern California coastline. The size and location of the earthquake prompted the National Weather Service to send out a tsunami warning to many of the 5.3 million people along the 500 miles of affected California and Oregon coastlines, advising them to move inland and towards higher ground. By approximately 11:45 a.m., the tsunami warning was canceled. Immediately following the 7.0 earthquake, the Bay Area Rapid Transit (BART) ceased operations, though they resumed operations around 12:00 p.m. with significant delays reported. At least 22 aftershocks between magnitudes 4.3 and 2.5 have hit Northern California since the 7.0, and the U.S. Geological Survey (USGS) has warned that "there is currently a 5% chance of a magnitude 6 or larger earthquake occurring in the next week, and a 34% chance of a magnitude 5 quake occurring in that time frame." California Governor Gavin Newsom signed a state of emergency declaration to allow funds to provide aid to affected areas as needed, though so far, the damage has been relatively minor and localized. Damage assessments are still being conducted throughout the affected areas. Large cracks have appeared on some local roads, one gas leak was reported, and structures in the area have experienced damage to roofs, foundations, windows, and objects inside. Multiple USGS resources regarding how to prepare for and act during earthquakes can be found at: <https://www.usgs.gov/faqs/what-should-i-do-during-earthquake>.

**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



## TERRORISM & EXTREMISM

### **Young People Involved In One-Fifth Of Australian Terrorism Cases, Intelligence Chief Says**

*Reuters, 12/3/2024*

[Australia] One in five priority counter-terrorism cases investigated by Australia involved youth, the country's spy chief said on Friday, as the "Five Eyes" intelligence partners warned about the radicalisation of young "digital natives". Mental health, education and social services needed to intervene in many cases before the behaviour of minors became a police issue, said a research paper by the Five Eyes, which also include the U.S., Canada, Britain and New Zealand. "Around 20% of ASIO's priority counter-terrorism cases involve young people. In every one of the terrorist attacks, disruptions and suspected terrorist incidents in Australia this year, the alleged perpetrator was a young person," Australian Security Intelligence Organisation (ASIO) Director-General Mike Burgess said in a statement. "As a parent, the numbers are shocking. As an intelligence officer, the numbers are sobering," he said. The Australian Federal Police (AFP) had investigated 35 teenagers aged 17 years or younger, including a 12-year-old, in terrorism investigations since 2020, said AFP Commissioner Reece Kershaw. Over half of them were charged with offences, he said. <https://www.reuters.com/world/asia-pacific/young-people-involved-one-fifth-australian-terrorism-cases-intelligence-chief-2024-12-05/>

### **Melbourne Synagogue Fire Condemned By PM As 'Act Of Hate', As Witnesses Describe Seeing Masked Attackers**

*ABC News Australia, 12/5/2024*

[Australia] Australian Jewish community leaders say "no-one should be surprised" following the arson attack on a Melbourne synagogue on Friday morning, and urged politicians to do more to address anti-Semitism they called a "stain on [the] nation". Fire crews were called to the Adass Israel Synagogue at Ripponlea in Melbourne's south-east shortly after 4am and found a large fire burning through the building. Early-morning worshippers inside the synagogue reported seeing two masked men throw fuel inside the premises, before setting it alight. "There was some banging on a door with some liquid thrown inside and was lit alight, the few people inside the synagogue ran outside the back door, one of them got burnt," Adass Israel Synagogue board member Benjamin Klein said. <https://www.abc.net.au/news/2024-12-06/melbourne-synagogue-fire-adass-israel-community-suspicious/104692108>

**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



## SECURITY & SAFETY AWARENESS

### **Gunman Who Shot 2 Kindergartners At A California School Wrote About Attack Targeting Children** *Associated Press, 12/5/2024*

[California] A gunman who critically wounded two kindergartners at a tiny religious school in Northern California was mentally ill and believed by targeting children he was carrying out “counter-measures” in response to America’s involvement in Middle East violence, a sheriff said Thursday. Glenn Litton used a “ruse” of pretending to enroll a fictitious grandson to gain entry to the Feather River School of Seventh-Day Adventists in Oroville, Butte County Sheriff Kory L. Honea said during a news conference. Litton used a handgun to shoot two kindergarten boys, ages 5 and 6, who remained in critical condition Thursday, the sheriff said. Litton then used the weapon — a so-called ghost gun, which is difficult for investigators to trace — to kill himself just yards (meters) from the school’s playground. While Honea said Litton, 56, also had a lengthy criminal history — mostly theft and identity theft — authorities said they did not find any violent crimes on his record. <https://apnews.com/article/butte-county-california-school-shooting-1a183fcd1670d47dedeff81d9f1ce492>

### **Germany To Push For Autonomous Vehicles In Public Transport, Freight** *dpa, 12/4/2024*

The German government approved on Wednesday a strategy paper encouraging the use of autonomous vehicles for public transportation and goods delivery. The aim is to create the world's largest single-operating area for autonomous vehicles in Germany by 2028. While Germany is already a pioneer in the field of autonomous vehicles from a legal standpoint after laws passed in 2017, 2021 and 2022, the country lags behind some parts of the world in terms of operation. Whereas US cities such as San Francisco and Phoenix, as well as some in China, have well-established robo-taxi services, Germany is limited to individual pilot projects, without a scalable business model. Transport Minister Volker Wissing said autonomous driving should be deployed across Germany in the future. <https://www.yahoo.com/news/germany-push-autonomous-vehicles-public-171306057.html>

**ANALYST COMMENTARY:** On 4 December 2024, the German government adopted a strategy that furthers their government initiatives towards implementing autonomous vehicles on their roadways. The German government has been working on frameworks and guidelines that would allow the use of autonomous vehicles on their roadways since 2015, and multiple German studies referenced in the latest strategy found that “there is potential for promising use cases for autonomous driving in both local public transport and freight transport.” The strategy applies to all autonomous driving vehicles, though is heavily oriented towards autonomous freight and public transportation. It promotes innovation within Germany in hopes that German manufacturers will contribute to the creation of autonomous driving technology, and also suggests the implementation of autonomous driving will be done with hefty feedback from German citizens to ensure they are comfortable with the changes.

**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



Multiple firms are conducting self-driving/autonomous vehicles testing and operations within the U.S. currently, including Waymo, which offers limited “robotaxi” services in Phoenix, Arizona and San Francisco, California. Waymo also operates approximately 48 autonomous Class 8 trucks (trucks weighing over 33,000 pounds) across the U.S. that have human drivers on board to ensure safe operations. While Waymo’s autonomous vehicles have been involved in a number of incidents, ranging from “erratic” behavior like stopping at green lights to accidentally crashing into cyclists and other vehicles, Waymo reports that during the first 7.1 million miles driven autonomously, Waymo vehicles were only involved in three crashes with injuries, which means human-operated cars are four to seven times more likely to be involved in injurious crashes than Waymo vehicles involved in the study. That being said, Waymo vehicles are often the targets of vandalism, sabotage, and harassment, the motivations of which are not always clear. For years, Waymo vehicles in San Francisco have been waylaid by criminals and been graffiti’d, caught on fire, had their tires slashed, or been otherwise impeded on numerous occasions. In 2023, one particular group of “activists” began placing traffic cones on autonomous vehicles in San Francisco to “trick” their sensors and render the vehicles inoperable. The full strategy approved by the German government (written in German) can be found at: [https://bmdv.bund.de/SharedDocs/DE/Publikationen/DG/die-zukunft-faehrt-autonom.pdf?\\_\\_blob=publicationFile](https://bmdv.bund.de/SharedDocs/DE/Publikationen/DG/die-zukunft-faehrt-autonom.pdf?__blob=publicationFile)

## CYBERSECURITY

### FBI Warns iPhone And Android Users—Stop Sending Texts

*Forbes, 12/5/2024*

Timing is everything. Just as Apple’s adoption of RCS had seemed to signal a return to text messaging versus the unstoppable growth of WhatsApp, then along comes a surprising new hurdle to stop that in its tracks. While messaging Android to Android or iPhone to iPhone is secure, messaging from one to the other is not. Now even the FBI and CISA, the US cyber defense agency, are warning Americans to use responsibly encrypted messaging and phone calls where they can. The backdrop is the Chinese hacking of US networks that is reportedly “ongoing and likely larger in scale than previously understood.” Fully encrypted comms is the best defense against this compromise, and Americans are being urged to use that wherever possible. <https://www.forbes.com/sites/zakdoffman/2024/12/05/fbi-warns-iphone-and-android-users-stop-sending-texts/>

### Compromised Software Code Poses New Systemic Risk To U.S. Critical Infrastructure

*Security Infowatch, 12/4/2024*

The code that makes up the software now powering U.S. utilities is rife with vulnerabilities, including hundreds that are “highly exploitable,” a new research report released by Fortress Information Security today finds. Researchers studied thousands of products and found troubling risk patterns. The report, Beyond the Bill of Materials: The Silent Threat Lurking in Critical Infrastructure Software, also shows that

## 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



25 percent of software components and 90 percent of software products contained code from developers in China. Compromised software code can provide threat actors with a "backdoor" into power grids, oil and gas pipelines, and communication networks. In similar research last year, Fortress discovered that code developed in China was 1.4 times more likely to contain vulnerabilities than code developed elsewhere. <https://www.securityinfowatch.com/critical-infrastructure/press-release/55247530/fortress-cyber-security-compromised-software-code-poses-new-systemic-risk-to-us-critical-infrastructure>

## **New Android Spyware Found On Phone Seized By Russian FSB**

*Bleeping Computer, 12/5/2024*

After a Russian programmer was detained by Russia's Federal Security Service (FSB) for fifteen days and his phone confiscated, it was discovered that a new spyware was secretly installed on his device upon its return. The programmer, Kirill Parubets, was arrested by the FSB after being accused of donating to Ukraine. After regaining access to his mobile device, the programmer suspected it was tampered with by the Russian government after it exhibited unusual behavior and displayed a notifications stating, "Arm cortex vx3 synchronization." After sharing it with Citizen Lab for forensic analysis, investigators confirmed that spyware had been installed on the device that impersonated a legitimate and popular Android app 'Cube Call Recorder,' which has over 10,000,000 downloads on Google Play.

<https://www.bleepingcomputer.com/news/security/new-android-spyware-found-on-phone-seized-by-russian-fsb/>

**ANALYST COMMENTARY:** The case of Kirill Parubets highlights the Russian FSB's evolving use of advanced spyware for surveillance and repression. The spyware found on his phone, suspected to be a revamped version of Monokle, represents a significant leap in capability, exploiting permissions to grant extensive access to sensitive data and system functions. Unlike the original Monokle, this variant improves upon encryption, making detection and analysis more challenging. Its ability to monitor calls, capture keystrokes, and extract stored passwords demonstrates a tailored approach for maximum surveillance efficiency, targeting both communications and device integrity. The choice to disguise the malware as a legitimate app like Cube Call Recorder is a calculated move, leveraging the trust users place in widely downloaded apps to bypass suspicion. The spyware's expanded permission set, including background location tracking and package installation, reflects an intent to enhance stealth and persistence. The potential for an iOS version further broadens the threat landscape, underscoring the adaptability of the operators behind this tool. This incident reinforces the risks associated with device confiscation in high-risk environments. Individuals in similar situations should regard returned devices as compromised and consider replacing them entirely. Using temporary "burner" devices, maintaining strict operational security, and employing features like Lockdown Mode can help mitigate such threats. For organizations, this case signals the need to train employees on these risks and establish protocols for responding to suspected tampering, especially when dealing with state-level adversaries.

**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: 877-847-5510 or email [mcanalyst@motorcoachisac.org](mailto:mcanalyst@motorcoachisac.org)