Information Sharing & Analysis Center

PUBLIC TRANSPORTATION, OVER THE ROAD BUS, & SURFACE TRANSPORTATION

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

December 4, 2024

SUSPICIOUS ACTIVITY & INCIDENT REPORTS

No Arrests After 2 Shot Near South Dallas DART Station
FOX 4, 12/3/2024

[Dallas, Texas] wo people were hospitalized after a shooting near a DART station in South Dallas. The shooting happened around 4 p.m. Tuesday. Dallas police say a man and woman were found shot near South Boulevard and Meadow Street near the DART MLK Jr. station. They were both taken to a nearby hospital in unknown conditions. No suspects have been arrested, and police did not release a description. https://www.fox4news.com/news/no-arrests-after-2-shot-near-south-dallas-dart-station

Minivan Driver Seriously Injured in Collision with MBTA Train in Abington, Rail Service Disrupted
Hoodline, 12/3/2024

[Abington, Massachusetts] An MBTA Commuter Rail train collided with a minivan in Abington, Massachusetts, resulting in serious injuries for the driver and causing significant delays on that rail line. The accident, which took place yesterday afternoon, saw first responders rushing to the scene to aid the 45-year-old female driver, who was subsequently taken to a hospital for treatment, as stated by NBC Boston. The collision occurred at a railroad crossing near the junction of Railroad Street and North Avenue. Video footage provided by WCVB shows the destroyed minivan lying in a ditch beside the train. The incident took place just after 3 p.m. Witnesses reported that it appeared the minivan's driver went around a crossing gate and then stopped on the tracks. Brian Baker, an eyewitness, recounted the train conductor's attempts to halt the train, remarking that the train conductor "did everything he could do to slow the train down. All the way from that intersection, he locked it up, train was shaking, he did a great job." https://hoodline.com/2024/12/serious-injuries-for-minivan-driver-after-collision-with-mbta-commuter-train-in-abington-rail-service-disrupted/

FBI Seeks Public's Help After Reports Of Drones Flying Around Morris County, New Jersey
ABC 6, 12/4/2024

[Morris County, New Jersey] The FBI and New Jersey State Police are now asking for any public information after reports of drones seen flying around Morris County last week. The drones were reported flying in several areas along the Raritan River. "Law enforcement has been notified for the last week or so about people seeing drones mostly at night," said Washington Township Mayor Matt

Murello. The nightly drone sightings involved larger-than-hobbyist type drones and raised questions because of their proximity to both the Picatinny Arsenal and President-elect Trump's Bedminster golf course. A video obtained by WABC-TV from Bridgewater native Stephanie Marie shows other drones flying without noise and described about six feet across the sky with lights. https://6abc.com/post/nj-drone-investigation-fbi-state-police-seek-publics-help-after-activity-flying-around-morris-county/15621865/

ANALYST COMMENTARY: Beginning on 18 November 2024, witnesses began reporting suspicious nighttime drone activity in Morris County, New Jersey. Since then, the drones have been spotted multiple times in various locations across the county, including near Picatinny Arsenal, which houses the United States Army Combat Capabilities Development Command Armaments Center (CCDCAC), which conducts research and development for munitions, and the towns of Mendham and Parsippany. It is unclear who is operating the drones and what their motivations may be. Witnesses have reported that there are multiple drones operating together, with the Federal Bureau of Investigation (FBI) claiming witnesses reported seeing a "cluster" of drones accompanied by a larger fixed-wing aircraft. The New York Post has reported that the drones appear to be operating in two groups and have been seen over the Raritan River almost every night. Federal, state, and local agencies are investigating the incidents, though law enforcement have said there is no threat to the public. In December 2023, mysterious drones were also spotted operating near Langley Air Force Base in Virginia for 17 straight days. In the Langley instance, witnesses observed small drones operating in groups that appeared to be working in conjunction with a larger fixed wing aircraft at a higher altitude. The perpetrators and motives of the Langley incident was never released; however, a few weeks after the Langley incident, a Chinese exchange student was arrested and convicted on espionage charges for using a drone to spy on a U.S. naval facility nearby.

Four Trucks Destroyed In Suspicious Blaze At Transport Company In Oss
NL Times, 12/1/2024

[Oss, Netherlands] A fire early Sunday morning destroyed four trucks and a trailer at a transport company in Oss, with authorities suspecting arson. The blaze, which broke out around 1:30 a.m. at Van Bakel transport company on Tubantenweg, also damaged the company's building. No one was injured, including several people who were sleeping in a nearby building, which could have been impacted by the flames. Firefighters responded to the scene shortly after receiving the alarm, but by the time they arrived, the fire had already engulfed the vehicles. Despite efforts to control the blaze, the four trucks and trailer were completely destroyed, while two other trucks were saved after being moved in time. … Authorities are investigating the cause of the fire and suspect arson. Police have reviewed footage from surveillance cameras, which shows two individuals walking away from the scene shortly after the fire began. "At the moment the fire broke out, they were walking away from the area," the police stated. They are now searching for the suspects and have called on the public to provide any relevant information. https://nltimes.nl/2024/12/01/four-trucks-destroyed-suspicious-blaze-transport-company-oss

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

TERRORISM & EXTREMISM

UK Sanctions Northern Ireland Man Under Domestic Counter-Terrorism Laws
Reuters, 12/3/2024

[UK] Britain used counter-terrorism laws to freeze the assets of a man from Northern Ireland, citing his suspected involvement with "terrorist activity" associated with the New Irish Republican Army, a statement on Tuesday said. The government said it had "reasonable cause" to suspect that the individual, Brian Sheridan, who was born in Armagh, was involved in terrorist activity by facilitating terrorism and associating with members of the New IRA, as well as making funds available for the organization. The New IRA is one of a small number of active militant groups opposed to Northern Ireland's 1998 peace deal. It has been behind some of the sporadic attacks that have continued, including the murder of journalist Lyra McKee in 2019. "This action is the first use of the Treasury-led domestic counter terrorism financial sanctions regime targeting Northern Ireland related terrorism," Economic Secretary to the Treasury Tulip Siddiq said. https://www.reuters.com/world/uk/uk-sanctions-individual-under-n-ireland-related-counter-terrorism-laws-2024-12-03/

SECURITY & SAFETY AWARENESS

People Evading Transit Fares Totals $407K In Lost Revenue This Year
Sudbury.com, 12/4/2024

[Ontario, Canada] So far this year, fare evasion has cost the city's public transit system approximately $407,000. This figure, representing approximately 101,750 incidents based on $4 single-ride fares, was shared during Monday's 2025 budget meeting of city council, at which the city's elected officials approved hiring two part-time municipal law-enforcement officers to ride public transit. "Our bus operators are not instructed to enforce this themselves, and that is to ensure their own safety and well-being," city Transit Services acting manager Laura Gilbert told city council. A business case proposing the municipal law-enforcement officers also notes, "onboard issues are not considered by police in the absence of a significant/identified threat." City staff have tracked fare evasion by route and the times of day incidents have taken place and will schedule municipal law-enforcement officers accordingly. https://www.sudbury.com/city-hall/people-evading-transit-fares-totals-407k-in-lost-revenue-this-year-9900137

Why Experts Are Calling on Congress and Agencies to Improve Rail Safety
National Academies, 12/2/2024

Nearly every industry in the U.S. relies on the "steel backbone" of the country — its rail network. Freight trains transport raw materials like lumber, ore, and sand; intermediate goods such as paper pulp, chemicals, and metal; and finished products including toilet paper, toys, and food. High-profile derailments in recent years, notably in East Palestine, Ohio, have raised concerns, including about

whether safety in the industry is being sacrificed for the sake of speed and efficiency. In response to a request from Congress, a new National Academies report assesses the challenges that arise from operating longer freight trains, including derailments, blocked highway-rail grade crossings, and Amtrak delays. … we did not find that long trains are always more dangerous or that train size should be regulated. We did conclude, however, that there are heightened operational challenges and risks from increasing the length of manifest trains — and that these risks need to be recognized and addressed in a systematic way. Longer manifest trains with poorly positioned cars and locomotives have an increased risk of derailment. So, this change toward operating more long manifest trains has resulted in increased incidents and impacts on the public. https://www.nationalacademies.org/news/2024/12/why-experts-are-calling-on-congress-and-agencies-to-improve-rail-safety

NATO To Boost Efforts To Counter Russian, Chinese Sabotage Acts
Reuters, 12/3/2024

NATO will step up intelligence sharing and improve the protection of critical infrastructure in the face of "hostile" acts of sabotage against allies by Russia and China, NATO chief Mark Rutte said on Tuesday. Over the past years, Russia and China have tried to destabilize our nations with acts of sabotage, cyberattacks, disinformation and energy blackmail to intimidate us," Rutte told reporters. “NATO allies will continue to stand together to face these threats through a range of measures, including greater intelligence sharing and better protection of critical infrastructure," he said. NATO foreign ministers gathering in Brussels this week are expected to produce a new strategy to counter hybrid threats - a term that covers propaganda, political interference, deception, sabotage of key infrastructure, and other tactics beyond the conventional military domain. "There is a sustained, ongoing, daily hybrid campaign taking place against NATO allies," a senior NATO official told reporters on Tuesday.
https://www.reuters.com/world/nato-boost-efforts-counter-russian-chinese-sabotage-acts-2024-12-03/

South Korea Lifts President’s Martial Law Decree After Lawmakers Reject Military Rule
Associated Press, 12/3/2024

[South Korea] The president of South Korea early Wednesday lifted the martial law he imposed on the country hours earlier, bending to political pressure after a tense night in which troops surrounded parliament and lawmakers voted to reject military rule. President Yoon Suk Yeol, who appeared likely to be impeached over his actions, imposed martial law late Tuesday out of frustration with the opposition, vowing to eliminate “anti-state” forces as he struggles against opponents who control parliament and that he accuses of sympathizing with communist North Korea. Police and military personnel were seen leaving the grounds of parliament following the bipartisan vote to overrule the president, and the declaration was formally lifted around 4:30 a.m. during a Cabinet meeting. Parliament acted swiftly after martial law was imposed, with National Assembly Speaker Woo Won Shik declaring that the law was “invalid” and that lawmakers would “protect democracy with the people.”
https://apnews.com/article/south-korea-yoon-martial-law-997c22ac93f6a9bece68454597e577c1

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

CYBERSECURITY

Chinese Hackers Still Lurk In US Telecommunications Systems
Voice of America, 12/3/2024

Chinese hackers blamed for compromising U.S. telecommunications infrastructure and spying on American presidential campaigns and American officials are still entrenched in those systems, according to senior U.S. officials who warn it could be years before the hackers are kicked out. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the FBI on Tuesday urged U.S. telecommunication companies and their customers to take additional precautions, saying the breach might go deeper than first thought. "We cannot say with certainty that the adversary has been evicted because we still don't know the scope of what they're doing," Jeff Greene, CISA's executive assistant director for cybersecurity, said during a briefing with reporters. … The Chinese-linked hackers have been coy, adjusting their behavior as more information about their activities becomes public.
https://www.voanews.com/a/chinese-hackers-still-lurk-in-us-telecommunications-systems/7886221.html

ANALYST COMMENTARY: In September 2024, the Wall Street Journal reported that a People's Republic of China (PRC) affiliated cyber threat actor known as SaltTyphoon had breached multiple U.S. internet service providers in 2024. SaltTyphoon has been around since 2020 and has been positively linked to the PRC's Ministry of State Security (MSS), which is a massive Chinese intelligence agency with an incredibly broad mission and far-reaching jurisdiction. The MSS does not have a direct counterpart with any U.S. intelligence agency because they specialize in both foreign and domestic espionage and security activities. In October 2024, while investigating SaltTyphoon's breach of U.S. internet providers, U.S. security officials found that SaltTyphoon had exploited backdoors in the service provider's systems that were in place to provide U.S. law enforcement agencies with a method to conduct court-authorized wiretaps. Bruce Schneier, a computer security expert, has suggested that the hackers may have gained access through "one of the intermediary companies that sit between the government CALEA requests and the broadband providers," rather than through the broadband providers themselves. On 3 December, U.S. agencies claimed that the extent of the SaltTyphoon intrusion may be deeper than initially thought and warned U.S. telecommunication companies and their customers to take precautions. Experts believe that the PRC motive behind the cyber-attack was primarily to "[intercept] audio of phone calls and the content of text messages for a select number of high-profile U.S. government officials, such as individuals with the Trump and Harris campaigns." China has denied involvement, and when questioned about SaltTyphoon, a spokesperson for the Chinese Embassy in Washington, D.C. claimed that '"China firmly opposes and combats all kinds of cyber-attacks."

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

New NachoVPN Attack Uses Rogue VPN Servers To Install Malicious Updates
Bleeping Computer, 11/26/2024

A set of vulnerabilities dubbed "NachoVPN" allows rogue VPN servers to install malicious updates when unpatched Palo Alto and SonicWall SSL-VPN clients connect to them. AmberWolf security researchers found that threat actors can trick potential targets into connecting their SonicWall NetExtender and Palo Alto Networks GlobalProtect VPN clients to attacker-controlled VPN servers using malicious websites or documents in social engineering or phishing attacks. Threat actors can use the rogue VPN endpoints to steal the victims' login credentials, execute arbitrary code with elevated privileges, install malicious software via updates, and launch code-signing forgery or man-in-the-middle attacks by installing malicious root certificates. SonicWall released patches to address the CVE-2024-29014 NetExtender vulnerability in July, two months after the initial May report, and Palo Alto Networks released security updates today for the CVE-2024-5921 GlobalProtect flaw, seven months after they were informed of the flaw in April and almost one month after AmberWolf published vulnerability details at SANS HackFest Hollywood. https://www.bleepingcomputer.com/news/security/new-nachovpn-attack-uses-rogue-vpn-servers-to-install-malicious-updates/

ANALYST COMMENTARY: The NachoVPN vulnerabilities represent a critical threat to enterprise VPN security because it enables attackers to exploit unpatched Palo Alto GlobalProtect and SonicWall NetExtender clients. By tricking users into connecting to rogue VPN servers, attackers can install malicious updates, steal credentials, execute code with elevated privileges, and conduct man-in-the-middle attacks via forged root certificates. This is particularly dangerous for enterprises, as VPNs are gateways to sensitive internal resources. AmberWolf's release of NachoVPN, a simulation tool for rogue VPN server attacks, raises awareness but also amplifies the risk for unprepared organizations, as it provides a proof-of-concept for adversaries. The tool's platform-agnostic nature and extensibility could lead to the exploitation of additional VPN clients. For defenders, this shows the urgency of patching vulnerabilities. SonicWall's patch for CVE-2024-29014 (NetExtender) was issued months after the issue was identified, and Palo Alto only recently addressed CVE-2024-5921 (GlobalProtect), seven months post-disclosure. Organizations using these clients should update to the latest versions—NetExtender 10.2.341+ and GlobalProtect 6.2.6+—immediately. Enabling mitigations like FIPS-CC mode in GlobalProtect can provide an extra layer of defense. Additionally, implementing strong phishing defenses, network segmentation, and continuous monitoring can help mitigate the risk of rogue server attacks. AmberWolf's detailed advisories are a valuable resource for understanding the vulnerabilities and implementing protections, but proactive patching and vigilance remain paramount to counter these evolving threats.