Information Sharing & Analysis Center

PUBLIC TRANSPORTATION, OVER THE ROAD BUS, & SURFACE TRANSPORTATION

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

December 27, 2024

SUSPICIOUS ACTIVITY & INCIDENT REPORTS

At Least Three Killed & Four Seriously Hurt After Packed Bus 'With Tourists On Board' Plunges Into Lake In Norway
The Sun, 12/26/2024

[Norway] AT least three passengers have reportedly been killed after a packed bus plunged into a lake in Norway. The bus was said to be carrying 58 passengers - including "many foreign nationals" - when it skidded off a main road during bad weather. The vehicle was travelling on the E10 in Hadsel in Nordland county when it crashed through a barrier and into a lake. There had been reports of heavy snow drifts and strong winds in the area. Are Eilertsen from Nordland Police said three people have been confirmed dead so far and at least four are seriously injured. Many passengers are foreign nationals, according to local reports. Martin Reberg, general manager of Boreal Buss AS - a Norwegian bus company - confirmed the crash involved one of their vehicles, VG reports. It was on a trip from Narvik to Lofoten. Rescue leader Ørjan Delbekk told VG the bus is partially underwater and the extent of the damage is not yet clear. He said a large rescue operation is underway - with helicopters sent from nearby cities and volunteers from the Red Cross. https://www.the-sun.com/news/13162770/three-dead-bus-tourists-lake-norway/

3 Shot, 1 Stabbed In Christmas Night Dispute At Phoenix Sky Harbor Airport, Police Say
CBS News, 12/26/2024

[Phoenix, Arizona] Gunfire at Phoenix Sky Harbor International Airport on Christmas night left three people wounded, police say. Another person was stabbed. One was in critical condition. Then there was a second incident involving firearms, authorities said. According to police, officers responded to reports of gunfire at about 9:45 p.m. local time at a restaurant in Terminal 4 outside a security checkpoint and found a woman and two men suffering from gunshot wounds. All were hospitalized. The woman's condition was listed as life-threatening. The men were in stable condition. Officers then detained a man and juvenile female in a parking garage. He was taken to a hospital with at least one stab wound and was listed in stable condition. There was no initial indication that she was wounded. Police say early information was that the people involved all knew each other and were "engaged in a physical altercation that escalated" when one produced a gun. https://www.cbsnews.com/news/3-shot-1-stabbed-christmas-night-dispute-phoenix-sky-harbor-airport/

Undersea Cable Disruption In Baltic Sea Investigated For Possible Sabotage
Techspot, 12/26/2024

[Europe] Another undersea cable in the Baltic Sea has been disrupted. At around 12.26 pm local time on Christmas Day, the Estlink 2 power cable linking Finland and Estonia experienced an outage. Finland said sabotage could not be ruled out as a cause. Finland's prime minister, Petteri Orpo, said the outage had not affected the country's electricity supplies. However, Reuters reports that the capacity between the countries was reduced from the installed capacity of 1,016 MW to 358 MW. "The authorities remain vigilant even during Christmas and are investigating the situation," Orpo wrote on X. According to Finnish public broadcaster Yle, Estlink 2 was unserviceable for several months earlier this year due to planned maintenance, but the connection was restored in September. Arto Pahkin, Operations Manager of Finnish national electricity transmission operator Fingrid, said the possibility of sabotage cannot be ruled out, adding that an investigation into the matter had been initiated.
https://www.techspot.com/news/106097-undersea-cable-disruption-baltic-sea-investigated-possible-sabotage.html

Man Accused Of Striking RTA Bus Driver After Trying To Board Without Paying, Police Say
CBS News, 12/26/2024

[New Orleans, Louisiana] Police are asking for the public's help identifying and locating a man accused of striking an RTA bus driver after trying to board without paying. According to the New Orleans Police Department, the incident happened around 9:49 p.m. on Dec. 12. The man allegedly attempted to board an RTA bus at Canal and South Prieur Streets without paying the fare. When the bus driver and another employee intervened, the NOPD says the man struck the driver with and object and threatened to kill them both before fleeing. https://www.fox8live.com/2024/12/26/man-accused-striking-rta-bus-driver-after-trying-board-without-paying-police-say/

TERRORISM & EXTREMISM

Spain Faces Threats of Terrorism and Unrest, US Warns in Travel Advisory
Global Fight Against Terrorism Funding, 12/25/2024

[Spain] The U.S. Department of State is warning those thinking of traveling to Spain about dangers in that country. The department issued its travel advisory for Spain to Level 2 or "Exercise Increased Caution" — citing risks of terrorism and civil unrest on Monday. The advisory warns that terrorist groups may plan attacks there, potentially targeting tourist sites, transportation hubs, markets, government buildings, hotels, restaurants, places of worship, and other crowded public spaces. Such attacks could occur with little or no warning, the department said. The advisory also highlights frequent demonstrations, often tied to political or economic issues, significant holidays, or international events. Travelers are urged to avoid protests, stay vigilant in crowded areas, and follow instructions from local

authorities. https://www.gfatf.org/archives/spain-faces-threats-of-terrorism-and-unrest-us-warns-in-travel-advisory/

ANALYST COMMENTARY: The U.S. Department of State (DOS) guidance broadly aligns with assessments by other allied Western nations. According to the Canadian government's travel advice, violent crime is relatively rare in Spain, but petty crime is common. Demonstrations and strikes also happen regularly and can turn violent with little warning. Terrorism remains a threat across Europe as well. In its "Country Reports on Terrorism," DOS notes: "Spain continued to respond effectively to the global terrorism threat in border and transportation security, countering terrorism financing, and countering violent extremism through bilateral and multilateral cooperation… and temporarily reinforced its antiterrorism measures… following the onset of the Israel-Hamas conflict." However, terrorists have carried out attacks in several European countries, including in Spain. Per DOS, Spanish authorities continue "to arrest individuals suspected of planning terrorist attacks, facilitating terrorist financing, and engaging in [Islamic State Group (ISG)] and [al Qaeda]-related recruitment and radicalization both online and in their communities." Future terrorist attacks in Europe are likely. The national terrorism alert level for Spain is currently 'high,' indicating that indiscriminate attacks could occur anywhere at any time without warning. Spain's latest annual national security report concluded that "lone wolf attackers and self-radicalized cells" present the most persistent threat. Travelers in Spain are advised to maintain a heightened level of situational awareness in public spaces, particularly while attending sporting events or public celebrations and when near government buildings, places of worship, transportation hubs and networks, tourist attractions, restaurants, bars, coffee shops, shopping centers, markets, hotels, and other sites frequented by foreigners.

Boko Haram Terrorists Use Drones in Attack on Yobe Military Base
News Chronicle, 12/26/2024

[Nigeria] Suspected terrorists launched a drone attack on the 27 Task Force Brigade military base in Buni Gari, Yobe State, on Wednesday evening. Security sources revealed that the attackers used three drones in their attempt to strike the base. However, soldiers stationed there managed to shoot down all three drones after detecting unusual noises. "This appears to be the terrorists' latest tactic using drones. The attack happened around 5 p.m., but our troops were alert and acted swiftly to neutralize the threat," a source said. This incident comes less than 48 hours after a similar drone attack injured six soldiers at a Forward Operating Base (FOB) in Wajiroko, Damboa Local Government Area, Borno State. Reports indicate that on Monday, terrorists attacked the Wajiroko base using mortars and other weapons. Although the soldiers repelled the initial assault, the attackers returned shortly after with multiple armed drones carrying locally made grenades. https://thenews-chronicle.com/boko-haram-terrorists-use-drones-in-attack-on-yobe-military-base/

ANALYST COMMENTARY: The use of small unmanned aerial systems/drones by hostile threat actors in the U.S. has raised significant concerns regarding national security. The increasing accessibility of

drones worldwide has led to their adoption by global non-state actors for surveillance, reconnaissance, and attacks, with many global terrorist organizations and legitimate militaries weaponizing commercial off the shelf drones with explosive payloads and using them to strike targets. While U.S. based threat actors have not employed weaponized drones in any significant incidents leading to fatalities, there have been an increasing number of instances in which U.S.-based extremists, domestic terrorists, and other unknown actors have successfully used drones to carry out surveillance operations against national security interests and attempted to use drones to carry out kinetic attacks against critical infrastructure. In recent months, unknown actors have used drones to illegally surveil U.S. military installations in multiple states, and a Tennessee man was arrested for attempting to fly an explosive-laden drone into an electrical substation with the intent of causing widespread power outages. The U.S. government has responded to the growing threat of hostile drone usage in the U.S. with a series of mitigations, including funding anti-drone technologies such as surveillance programs aimed at detecting and intercepting drone threats and legislation restricting drone usage. However, challenges remain, such as the difficulty in distinguishing between legitimate drone activity and potential hostile actor use, as well as concerns over privacy and civil liberties. More information on protecting assets from drones can be found at: https://www.cisa.gov/sites/default/files/publications/Protecting%20Against%20the%20Threat%20of%20Unmanned%20Aircraft%20Systems%20November%202020_508c.pdf

SECURITY & SAFETY AWARENESS

Russia's 'Outrageous' Christmas Day Attack on Ukraine Triggers US Response
Newsweek, 12/26/2024

[Ukraine] Early on December 25, Russia attacked facilities propping up Ukraine's fuel and energy sector facilities, using both missiles and drones, according to Ukrainian authorities. In this image provided by the Ukrainian Emergency Service, firefighters put out a fire following a Russian missile attack on the country's energy system in Dnipropetrovsk region, Ukraine, Wednesday, Dec. 25, 2024. Moscow used 184 drones and missiles, Kyiv's air force said, including two North Korean-made KN-23 ballistic missiles, 12 Kalibr cruise missiles launched from the Black Sea, and more than 100 uncrewed aerial vehicles (UAVs). Ukraine intercepted 113 of the targets, including 55 cruise missiles and 54 drones, with another 52 UAVs failing to reach their intended locations, according to the air force. The attacks homed in on energy facilities across the country, including the northeast Kharkiv region, central Dnipropetrovsk and Poltava areas and Ivano-Frankivsk, in western Ukraine. Russia said it had targeted "critical power infrastructure facilities ensuring operation of Ukrainian defense industry enterprise," and that the objectives of the strike had "been achieved." https://www.newsweek.com/russia-christmas-day-missile-drone-attack-ukraine-us-military-aid-2006089#

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

As 'Smart Cities' Tools Grow Nationwide, So Do Privacy And Ethical Concerns
Louisiana Illuminator, 12/26/2024

After nearly a week of searching for a suspect in the hit-and-run death of an 81-year-old St. Helena, California, woman this summer, police found and arrested a man with the help of license plate reading cameras that registered him near the scene. The police department used information from FLOCK's automatic license plate reading camera system, which monitors and records license plate data in a cloud-based database. The company makes cameras, drones, audio detection and software tools used by cities, law enforcement and school systems with the goal of crime detection and faster solve times. Using a license plate number to find a suspect isn't new to crime solving, but finding that license plate in an autonomously-captured and organized data log, rather than by humans looking through security footage or searching in-person, is more novel. https://lailluminator.com/2024/12/26/smart-cities/

Waymo Dominated U.S. Robotaxi Market In 2024, But Tesla And Amazon's Zoox Loom
NBC, 12/26/2024

Despite General Motor's decision to shutter its Cruise robotaxi business earlier this month, the U.S. has never been closer to a driverless future. For the autonomous vehicle industry, 2024 will be remembered as the year that at least one major U.S. player -- Alphabet-owned Waymo -- saw glimmers of mainstream adoption and made strides toward commercial viability. That came after a rocky start for the self-driving car industry domestically. … A big focus for Waymo in 2025 will be expanding its robotaxi service to more cities, winning over riders and continuing research and development on newer technology that will allow the company's AVs to operate in more weather and traffic conditions. Waymo plans to launch a commercial service in Austin, Texas, and Atlanta, with rides available through the Uber app next year. It's also begun testing in Miami with plans to offer rides to the public there in 2026. https://www.nbcnews.com/business/autos/waymo-dominated-us-robotaxi-market-2024-tesla-amazons-zoox-loom-rcna185458

ANALYST COMMENTARY: Autonomous vehicles (AVs) are rapidly emerging as a transformative technology in the U.S., with major companies like Tesla, Waymo, and Uber testing self-driving cars. Proponents of AVs claim their usage will improve road safety, reduce traffic congestion, and increase mobility for people with disabilities. However, their integration into society also raises significant concerns. One of the primary threats is cybersecurity. As AVs rely on complex software, sensors, and communications networks, they become vulnerable to hacking and malicious cyber interference. Cyber-attacks could compromise vehicle control systems, causing accidents or allow threat actors to exploit vulnerabilities for terrorism or criminal activity. The risk of such attacks grows as AVs become more prevalent, add additional systems, and become more connected to broader smart city infrastructures, which significantly increases the number of attack surfaces the vehicles have. Another concern is the potential loss of jobs in sectors such as trucking and delivery services, where autonomous vehicles could replace human workers. There are also legal and ethical issues

surrounding autonomous driving. In the event of an accident, determining liability—whether with the manufacturer, software developers, or other parties—becomes complex. Additionally, ethical decisions, such as how an AV should react in what the computer perceives as an unavoidable crash scenario, raise concerns about programming and moral frameworks. As of now, there have been no widely reported instances of cyber criminals directly interfering with the operations of autonomous vehicles (AVs) in the U.S. in a way that results in significant harm. However, there have been several potential incidents involving AVs that highlight the vulnerabilities of autonomous systems, especially when it comes to cybersecurity and criminal activity. In multiple instances, researchers have demonstrated that existing vehicles with autonomous driving software can be "hijacked" through the use of sophisticated cyberattacks that gain access to the vehicles' navigation software and other critical systems required for safe vehicle operation and override user inputs. A comprehensive study detailing current vulnerabilities that have been exploited in self-driving vehicles and mitigation techniques that can be used to harden against known attack vectors can be found at: https://ieeexplore.ieee.org/document/9257492

Rail Vision Joins MxV Rail's Safety Technology Programme
Railway Technology, 12/26/2024

Rail Vision has announced its partnership with MxV Rail's Technology Roadmap Program to bolster the safety and efficiency of North American rail operations. The partnership with MxV Rail's program allows Rail Vision to work alongside top US rail operators, enhancing its visibility among potential customers. This move is significant for the company as it seeks to provide safety and automation solutions within the rail industry. Rail Vision CEO Shahar Hania said: "Rail Vision sees itself as a global influencer and is proud to join this prestigious US rail committee dedicated to supporting development of interoperable requirements for rail operations. "This membership allows us to collaborate with leading industry experts and expand our footprint in the US rail market. Being part of this consortium underscores our commitment to innovation and positions us as a key contributor to the advancement of technology in the North American rail environment." https://www.railway-technology.com/news/rail-vision-mxv-rail-technology-program/

CYBERSECURITY

Cybercriminals Exploit Google Calendar to Spread Malicious Links
Infosecurity Magazine, 12/17/2024

New research from Check Point has revealed how cybercriminals are bypassing email security measures by using Google Calendar and Drawings to send seemingly legitimate invites containing malicious links. The study highlighted how cybercriminals are bypassing email security policies that previously flagged malicious calendar invites. Many of the emails look legitimate because they appear to directly originate

from Google Calendar and the calendar files (.ics) include a link to Google Forms or Google Drawings. Check Point said that after observing that security products could flag malicious calendar invites, cybercriminals evolved the attack to align with the capabilities of Google Drawings. The malicious actors modify "sender" headers, making emails look as though they were sent via Google Calendar on behalf of a known and legitimate individual. The aim of the attack is to allow for the theft of corporate or personal information. https://www.infosecurity-magazine.com/news/cybercriminals-exploit-google/

ANALYST COMMENTARY: This attack method exploits the trust users place in Google's ecosystem and shows the evolving sophistication of phishing schemes. By leveraging Google Calendar and Drawings, attackers bypass traditional email security measures designed to detect malicious links. This method also capitalizes on the inherent legitimacy of Google domains, which can make it harder for security tools to flag these emails as suspicious. The use of reCAPTCHA-like elements or support buttons adds another layer of deception, as these are typically associated with security processes, further lulling victims into a false sense of safety. To mitigate these risks, organizations are encouraged to consider implementing additional security measures, such as domain-specific link scanning and behavioral analytics to detect unusual user interactions. Training users to scrutinize unexpected invitations and encouraging a "verify before you click" culture are also crucial. On the technical side, Google's "known senders" feature is a useful defense but not foolproof. Administrators should enable advanced phishing and malware protection in Google Workspace, block unfamiliar domain links, and use security tools that specialize in detecting emerging attack vectors. This attack also reflects a broader trend: cybercriminals weaponizing legitimate platforms to circumvent security tools. Awareness campaigns paired with robust technical controls can help organizations and individuals stay ahead of such evolving threats.