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

November 5, 2024

CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE (CISR) MONTH

Security And Resiliency Guide: Counter-Improvised Explosive Device (C-IED) Concepts, Common Goals, And Available Assistance

The Security and Resiliency Guide: Counter-IED Concepts, Common Goals, and Available Assistance (SRG C-IED) is intended to help communities, individual organizations, and facility owner/operators plan and implement C-IED activities within their overall public safety and emergency management approach. You can use it to understand the IED risk landscape in the U.S. and your locale; apply common IED-specific security and resiliency goals; and leverage available U.S. Government resources to build and sustain preparedness. The SRG C-IED was created by the Department of Homeland Security in coordination with the Federal Bureau of Investigation, with contributions from IED and C-IED experts and stakeholders. https://www.cisa.gov/publication/security-and-resiliency-guide-and-annexes

SUSPICIOUS ACTIVITY & INCIDENT REPORTS

Man Arrested And Charged With Attempting To Use A Weapon Of Mass Destruction And To Destroy An Energy Facility In Nashville
Department of Justice, 11/4/2024

[Nashville, Tennessee] Skyler Philippi, 24, of Columbia, Tennessee, was arrested by federal agents and charged with attempting to use a weapon of mass destruction and attempting to destroy an energy facility. "As charged, Skyler Philippi believed he was moments away from launching an attack on a Nashville energy facility to further his violent white supremacist ideology – but the FBI had already compromised his plot," said Attorney General Merrick B. Garland. "Driven by a racially motivated violent extremist ideology, the Defendant planned to attack the power grid with a drone and explosives, leaving thousands of Americans and critical infrastructure like hospitals without power," said FBI Director Christopher Wray. https://www.justice.gov/opa/pr/man-arrested-and-charged-attempting-use-weapon-mass-destruction-and-destroy-energy-facility

ANALYST COMMENTARY: On 4 November 2024, the U.S. Department of Justice (DOJ) charged Skyler Philippi, age 24, of Columbia, Tennessee, with attempting to use a weapon of mass destruction and attempting to destroy an energy facility in Nashville, Tennessee. According to the DOJ, Philippi planned

NOT FOR PUBLIC DISSEMINATION

to affix an explosive device to an unmanned aircraft system (UAS or drone) and then fly the explosive laden drone into an energy facility in furtherance of accelerationist ideology. According to the Federal Bureau of investigation (FBI), in June 2024 Phillipi told a confidential human source that he wanted to commit a mass shooting at a YMCA in Columbia, Tennessee, and the source alerted the FBI. In July 2024, Philippi shared his accelerationist ideology with a second human source reporting to the FBI, and told them, "If you want to do the most damage as an accelerationist, attack high economic, high tax, political zones in every major metropolis." During this time, Philippi also discussed the impact of targeting interstate electric substations and asked the second source for "assistance in stealing a train de-railer for the purpose of derailing a train in the Middle District of Tennessee." For his plot to attack the electric sector, Philippi conducted multiple reconnaissance trips to study his intended targets, including a preoperational reconnaissance mission he conducted alongside the FBI sources in late September 2024. Philippi told the FBI sources that he intended to build a drone for the attack himself with 3D printed parts, though this proved too difficult and he ultimately weaponized a drone supplied to him by one of the FBI sources. Philippi was also supplied with inert pipe bombs by an FBI source, and during the evening of 2 November, the FBI sources accompanied Philippi to the area he intended to launch the drone for his attack, and Philippi asked them to serve as his security detail why he carried out his attack. He also took a firearm with him and told the FBI sources that he intended to shoot law enforcement if confronted. When asked if he was sure he wanted to go through with the attack, Philippi responded that he was "fully committed" and that it was "time to do something big" that would be remembered "in the annals of history." Philippi was arrested while attaching what he believed was a live pipe bomb to a drone moments before he planned to crash the drone into the substation. It is unclear how he intended to steal a de-railer, or what his potential target for the de-railer would have been had he acquired one.

Man Stabbed At King Memorial MARTA Station, Police Say
Atlanta News First, 11/4/2024

[Atlanta, Georgia] Police are investigating after a man was allegedly stabbed at a MARTA station in Fulton County. Officers responded to King Memorial MARTA station at around 8:16 p.m. Sunday. When they arrived, they found a 44-year-old with a "laceration," investigators said. The victim was taken to the hospital. Authorities believe there was some sort of argument between the victim and suspect that escalated. No arrest has been made at this time. The investigation remains ongoing.
https://www.atlantanewsfirst.com/2024/11/04/man-stabbed-king-memorial-marta-station-police-say/

Man Charged With Soliciting Sex From Teen At Spring Hill Metro Station
Fairfax County News, 11/4/2024

[Maryland] A Maryland man was arrested over the weekend after allegedly soliciting sex from a 15-year-old he met at the Spring Hill Metro station in Tysons. The teen's parents reported to the police on Friday (Nov. 1) that a man had solicited their child first in person and then in subsequent communications in

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.**

October, according to the Fairfax County Police Department. An investigation by detectives found that Logan Russell Farrell, 38, had allegedly approached the teen at the Metro station and offered money for sexual acts, the FCPD said in a press release. "Farrell at the time of the encounter was a stranger to the victim," police said. "Afterwards, Farrell continued communicating with the victim soliciting sexual acts and illicit pictures." https://www.ffxnow.com/2024/11/04/just-in-man-charged-with-soliciting-sex-from-teen-at-spring-hill-metro-station/

Woman Stabbed In Area Of Forest Hills MBTA Station
NBC 10, 11/4/2024

[Boston, Massachusetts] A woman was stabbed Monday afternoon near an MBTA station in Boston's Jamaica Plain neighborhood. Boston police say the incident happened just after 4:15 p.m. on Washington Street in the area of Forest Hills. The woman suffered life-threatening injuries, according to police. Authorities did not say whether any arrests have been made. The stabbing is under investigation. https://www.nbcboston.com/news/local/woman-stabbed-in-area-of-forest-hills-mbta-station/3540679/

TERRORISM & EXTREMISM

Man Arraigned Over Distribution Of Extremist Material Was Planning Terror Attack In France
Malta Today, 11/1/2024

[Mediterranean] A man arraigned over the alleged distribution of extremist material was planning to carry out a terrorist attack in France, a court heard on Friday. Mouhamadou Dosso, an Ivory Coast national, was arrested in an early-morning raid following intelligence linking him to extremist content and plans to carry out a terror attack. Dosso, a 32-year-old man from the Ivory Coast who works in maintenance, was arrested in a 5am operation on 31 October, Giovanni Barbara Street, Hamrun, in connection with the distribution of the extremist material. The discovery of such conversations led to the man's arrest, following weeks of surveillance and intelligence analysis in a coordinated effort among various sections of the Police Force.
https://www.maltatoday.com.mt/news/court_and_police/132082/man_arraigned_over_distribution_of_extremist_material_was_planning_terror_attack_in_france

30 Years Of Trends In Terrorist And Extremist Games
Global Network on Extremism & Technology, 11/1/2024

Violent extremist, terrorist, and targeted hate actors have been actively exploiting video games to propagandize, recruit and fundraise for more than 30 years. This report presents an analysis of that history using a unique dataset, the Extremist and Terrorist Games Database (ETGD), developed by the authors. It contains 155 reviewed entries of standalone games, modifications for existing games (mods) and browser-based games dating from 1982 to 2024. The titles analyzed appear across the ideological

spectrum: far right (101 titles), jihadist (24), far left (1) and other forms of extremism and targeted hate (29), including school-massacre ideation (12). They span platforms ranging from simple standalone games for Atari in the 1980s to sophisticated mods for some of today's most popular games. The number of titles has increased year on year – in line with global conflict and extremist ideological trends, and revealing a continued push by malicious actors to exploit gaming. https://gnet-research.org/2024/11/01/30-years-of-trends-in-terrorist-and-extremist-games/

SECURITY & SAFETY AWARENESS

US Ultimate Target For Russian Incendiary Devices Hidden On Jets, Say Officials
Aerotime, 11/5/2024

[Europe] Fires at cargo warehouses in Birmingham, United Kingdom, and Leipzig, Germany, caused by incendiary devices hidden in packages may have been part of a larger plan to target aircraft bound for the United States (US) and Canada. Russia is suspected of being involved in the plot to smuggle incendiary devices from Lithuania into the UK and Germany with the plan to target North America further in the future. The fires in Birmingham and Germany both broke out in July 2024, while stored in warehouses and had previously been transported on DHL cargo planes, according to the Wall Street Journal. It is understood that the package in Leipzig was also destined for the UK with both parcels due to be delivered to Birmingham addresses. https://www.aerotime.aero/articles/incendiary-devices-russia-plan-aircraft-warehouse-fire

ANALYST COMMENTARY: In July 2024, two parcels at DHL logistics centers in Birmingham, UK and Leipzig, Germany caught fire, prompting an international investigation that determined that the parcels contained explosives consisting of "electric massagers implanted with a magnesium-based flammable substance" and were sent to the UK from Lithuania. It is unclear how many explosive parcels were sent, though Lithuanian authorities arrested an individual believed to have sent four explosive parcels from Lithuania, and Poland's National Prosecutor's Office claims they have arrested four people in connection with the plot and are looking for two others. The individuals are accused of working as proxy forces for Russian spy services, and Polish authorities have said they believe that "the group's goal was also to test the transfer channel for such parcels, which were ultimately to be sent to the United States of America and Canada." The four people arrested in Poland have been charged "with participating in sabotage or terrorist operations on behalf of a foreign intelligence agency." Western officials have also alleged that Russia is behind the attacks, though it is unclear if the intent was for the devices to detonate while onboard airborne cargo or passenger aircraft, or while on the ground in logistics facilities. The Wall Street Journal has reported that unnamed security sources "believe that two incendiary devices, shipped via DHL, were part of a covert Russian operation that ultimately aimed to start fires aboard cargo or passenger aircraft flying to the U.S. and Canada," though this has not been confirmed publicly by any U.S. government official. On 4 November, a

Transportation Security Administration spokesperson remarking on the incidents said that TSA has added security measures for U.S. aircraft operators and foreign air carriers "regarding certain cargo shipments bound for the United States."

Pedestrian Bridges, RTC Bus Stops Affected By F1 Closures As Las Vegas Race Approaches
CBS 8, 10/25/2024

[Las Vegas, Nevada] Four pedestrian bridges along the Strip will be closed at night in the coming weeks as preparations continue for this year's F1 Las Vegas Grand Prix. Race organizers said the closures involve installation of enclosures to the bridges. The four bridges and details on closure times: The Cromwell to Caesars Palace: closed 9:00 p.m. to 9 a.m. on Nov. 3–6. Wynn Las Vegas to The Venetian/Palazzo (across Sands Avenue): closed 9:00 p.m. to 9:00 a.m. Nov. 3-6. The Venetian/Palazzo to Treasure Island: closed from midnight to 9:00 a.m. on Nov. 7-11. Planet Hollywood to Cosmopolitan: closed from midnight to 9:00 a.m. on Nov. 7-11. The pedestrian bridges will be closed overnight and will be open outside of these hours, officials said. https://www.8newsnow.com/news/local-news/pedestrian-bridges-rtc-bus-stops-affected-by-f1-closures-as-las-vegas-race-approaches/

Five Key Takeaways From the 2024 Commuter Rail Summit
Railway Age, 11/1/2024

[Boston, Massachusetts] Commuter railroads are moving beyond the traditional 9-5 commuter. The way people live, work, and play has changed and there appears to be no going back. Agencies are rethinking schedules, fares, partnerships, and customer amenities to reach and retain new riders. To explore the future of commuter rail and collaborate on the most pressing issues facing the industry, the Commuter Rail Coalition recently convened the 2024 Commuter Rail Summit in Boston. The in-person event brought together agency leaders and policymakers from across the country for a series of panel discussions, fireside chats, and technical tours. The third annual Summit explored topics ranging from just-in-time climate resiliency efforts to the coming fiscal cliff as pandemic-era funding sources run dry. https://www.railwayage.com/passenger/commuterregional/five-key-takeaways-from-the-2024-commuter-rail-summit/

ANALYST COMMENTARY: The 2024 Commuter Rail Summit took place between 14-16 October 2024 in Boston, Massachusetts. The event was hosted by the Massachusetts Bay Transportation Authority (MBTA) and featured presentations and discussions on technology, developments, and the future of commuter railroads. The event was attended by U.S. Rep. Jake Auchincloss, MBTA CEO Phillip Eng, and Mass. Transportation Secretary Monica Tibbits-Nutt, among other stakeholders. Kelly Anne Gallagher, CEO, of the Commuter Rail Coalition summarized the main topics of conversation and concern for the industry, which she provided to Railway Age. Gallagher noted that commute patterns and work habits have changed significantly since COVID-19 and commuter rail is evolving to meet the new norms. The traditional morning and evening rush hours are still present, but commuter rail is adding service for

weekends and late nights and the work week is no longer as traditional. There is also a renewed commitment to make public transportation available for a wider audience to alleviate the growing congestion in the inner cities. More frequent trains with a wider time service window is key to encouraging drivers to move to commuter rail. Los Angeles' MetroLink is investing heavily in expanding its service, in preparation for the 2028 Summer Olympics. Industry leaders also discussed fare structures, resiliency in operating during and following climate disasters and leveraging Artificial Intelligence (AI) and other technologies into operations.

CYBERSECURITY

White House Adviser Addresses Fleets' Need For Cybersecurity
Transport Topics, 10/29/2024

[Cleveland, Ohio] White House official Stephen Viña stressed the importance of trucking cybersecurity Oct. 28 even as carriers adapt to an unknown technological future. Viña, the assistant national cyber director for policy development at the Office of the National Cyber Director, discussed trucking companies' predicament at the National Motor Freight Traffic Association Cybersecurity Conference 2024. "I, and my colleagues at the White House, appreciate the critical importance of the transportation sector and specifically the work that you do in the trucking industry," Viña said. "But with that great responsibility comes a lot of expectations. Perhaps expectations that might not be fair." Viña highlighted how carriers are expected to have complete reliability and near-perfect predictability despite the inherent uncertainty in the market. But to meet that demand, carriers have deployed numerous technologies, such as telematics, Internet of Things sensors, electronic logging devices, 5G connectivity and artificial intelligence. This also means many vulnerabilities. https://www.ttnews.com/articles/nmfta-white-house-cybersecurity

Researchers Uncover Vulnerabilities In Open-Source AI And ML Models
The Hacker News, 10/29/2024

A little over three dozen security vulnerabilities have been disclosed in various open-source artificial intelligence (AI) and machine learning (ML) models, some of which could lead to remote code execution and information theft. The flaws, identified in tools like ChuanhuChatGPT, Lunary, and LocalAI, have been reported as part of Protect AI's Huntr bug bounty platform. The most severe of the flaws are two shortcomings impacting Lunary, a production toolkit for large language models (LLMs): CVE-2024-7474 (CVSS score: 9.1) - An Insecure Direct Object Reference (IDOR) vulnerability that could allow an authenticated user to view or delete external users, resulting in unauthorized data access and potential data loss; and CVE-2024-7475 (CVSS score: 9.1) - An improper access control vulnerability that allows an attacker to update the SAML configuration, thereby making it possible to log in as an unauthorized user and access sensitive information. https://thehackernews.com/2024/10/researchers-uncover-vulnerabilities-in.html

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION, OVER THE ROAD BUS, & SURFACE TRANSPORTATION

ANALYST COMMENTARY: The recent disclosure of vulnerabilities across multiple open-source AI and ML frameworks reveals significant security risks, particularly concerning remote code execution, data manipulation, and unauthorized access. In tools such as Lunary, LocalAI, and ChuanhuChatGPT, researchers have identified severe flaws, some with CVSS scores of 9.1, showcasing the high exploitation potential. For instance, Lunary's vulnerabilities (CVE-2024-7474 and CVE-2024-7475) involve insecure direct object references (IDOR) and improper access controls, enabling unauthorized data access and potential login as an admin user. Another IDOR vulnerability (CVE-2024-7473) in Lunary allows attackers to modify prompts by intercepting and manipulating user requests, creating risk for prompt hijacking in LLM-driven workflows. In ChuanhuChatGPT, a path traversal vulnerability (CVE-2024-5982) could permit arbitrary code execution, while LocalAI's flaws, including CVE-2024-6983, enable malicious configuration uploads that expose sensitive data and open avenues for timing attacks to deduce API keys. These vulnerabilities demonstrate a broader risk to AI/ML pipelines where user input can be leveraged for unauthorized actions. Protect AI's Vulnhuntr tool provides a proactive measure by identifying zero-day vulnerabilities in Python codebases, suggesting that more robust code analysis can mitigate these exposures early in development. The emergence of novel prompt-engineering tactics to jailbreak LLMs highlights how social engineering meets technical exploits; encoded prompts and emoji-laced payloads bypass input validation, allowing attackers to craft exploits indirectly. The findings show the need for comprehensive patching, robust code review, and advanced monitoring strategies to protect the AI/ML ecosystem against increasingly sophisticated threat vectors.

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.**