

To: SHRCOMMISSIONED[SHRCOMMISSIONED@piercecounitywa.gov]; SHRJCO[SHRJCO@piercecounitywa.gov]
Cc: David Hutchinson[david.hutchinson@piercecounitywa.gov]
From: Gary Smith
Sent: Fri 4/21/2023 2:56:31 PM
Subject: SSRIG Weekly Intelligence Summary 16 - 2023 (April 21, 2023)
Received: Fri 4/21/2023 2:56:42 PM
[SSRIG Weekly Summary 16-2023.pdf](#)

South Sound Regional Intelligence Group SSRIG email: PCINTEL@piercecounitywa.gov Weekly Summary	
#16-2023	April 21, 2023
Gary Smith Intelligence Analyst Gary.Smith@ci.tacoma.wa.us (253) 594-7964	
This document is a FOUO communication and is not to be disseminated outside of the law enforcement or intelligence communities. Dissemination to media sources is not authorized.	

REGIONAL

WA 2nd highest vehicle theft rate in US

OFFICER SAFETY

Attempt to Identify Drive-by Shooting/Assault 1st – Vehicle

Attempt to Identify Drive-by Shooting/Assault 1st - Vehicle and Person of Interest

OFFICER SAFETY / SITUATIONAL AWARENESS: Jack

OFFICER AWARENESS

BOLO; Smith

CYBER THREATS

A [Computer-Generated] Swatting Service Is Causing Havoc Across America

What it Will Look Like if China Launches Cyberattacks in the U.S.

PUBLIC SAFETY

(U) Upward Trend in Telephonic Hoax Active Shooter Threats to US Education Institutions Nationwide in 2023

NATIONAL

(U//FOUO) Transnational: New Eco-Extremist Publication Highlights Critical Infrastructure Vulnerabilities

(U) United States: Threat of Extremism in Online Video Game Communities

DHS Warns U.S. Extremists Pose Growing Threat to Cops, Reporters, Pipelines

INTERNATIONAL

Some U.S. Cities May Offer Model to Ease Canada Transit Violence: Experts


United States: (UPDATE) Justice Department Arrest Chinese Nationals Citing “Secret Police Station”

U.S. Adds Al Qaeda Leader in Syria to List of Global Terrorists

Other National/International Articles of Interest (Links):

Gary L. Smith

Gary L. Smith
Criminal Intelligence Analyst
Regional Intelligence Group
TPD/PCSD
Tacoma, WA
(253) 594-7964
(253) 405-6214 (C)
gary.smith@cityoftacoma.org
gary.smith@piercecountywa.gov

“There must be a Lone Ranger!” 

*** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY ***



TACOMA /PIERCE COUNTY REGIONAL INTELLIGENCE UNIT



16-2023

WEEKLY SUMMARY

Friday, April 21, 2023

Det. Sgt. John Delgado (253) 341-1369
john.delgado@pierccountywa.gov

Gary L. Smith, Intel Analyst
gary.smith@cityoftacoma.org (253) 594-7964

***** SENSITIVITY NOTICE *****

This document is intended exclusively for the individual or entity to which it is addressed. This communication may contain information that is law enforcement sensitive, proprietary, privileged, confidential and may be legally protected or otherwise exempt from disclosure. If you are not the intended recipient, you are hereby notified that any disclosure, dissemination, copying or distribution of this transmission is strictly prohibited. If you have received this message in error, please notify the sender immediately by email and delete all copies of this message.

**The SSRIG is a member of the Joint Terrorism Task Force. Agencies in Pierce County are encouraged to forward information first to The SSRIG and we'll be sure to forward the information accordingly.

Please treat this and all other communications from this Regional Intelligence Unit as **LAW ENFORCEMENT SENSITIVE**. Further distribution of this document is restricted to law enforcement agencies, intelligence agencies, and Department of Defense organizations only, unless prior approval of this office has been obtained.

THIS DOCUMENT OR ANY SEGMENT THEREOF, MAY NOT BE RELEASED TO ANY MEDIA SOURCES.

REGIONAL



WA 2nd highest vehicle theft rate in US

Car thefts in Washington state have been happening at a faster pace than most other states nationwide. Now the Evergreen State is also inching closer to being the state with the most vehicle thefts in America. It was previously reported that in 2022 Washington saw the third-highest number of vehicle thefts in the U.S., at 46,939, according to a report on thefts from the National Insurance Crime Bureau.

Every month, thousands of vehicles are snagged off the streets of Pierce and King Counties, the Puget Sound Auto Theft Task Force reports. But now, a new analysis shows that Washington has the second-highest rate of thefts per 1,000 vehicles. Vehicle history check platform carVertical reviewed the data from the NICB and found that for every 1,000 registered vehicles in Washington state, 15 were stolen in 2022. This equates to around one in every 67 registered vehicles stolen.

In addition to the NICB, carVertical collected data from government registries, insurance companies and other databases to uncover the total number of registered vehicles per state. The Evergreen State is tied for second with Missouri, both of which are eclipsed by Colorado's 28 vehicles stolen per 1,000 automobiles. California, which had around 202,685 vehicles stolen, had a slightly lower theft rate of 14 per 1,000 vehicles.

On top of the theft rates, carVertical also found that the nation's top five most-stolen vehicles are:

- Chevrolet Pick-Up – 48,206 stolen
- Ford Pick-Up – 47,999 stolen
- Honda Civic – 31,673 stolen
- Honda Accord – 30,274 stolen



*** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY ***

• Toyota Camry – 17,270 stolen

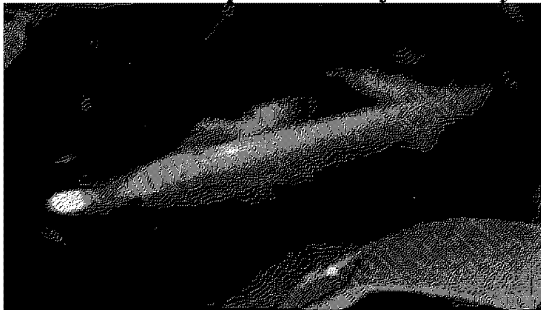
In April, Pierce County saw a slight increase in car thefts, at 771 compared to March's 748, per the Puget Sound ATTF's report. Law enforcement representatives previously told The News Tribune that trends on social media encouraging people to steal cars have directly impacted Washington's surge in stolen cars.

Vehicles that are the most susceptible to thefts include models from Hyundai and Kia. Over the past few months, the Puget Sound ATTF has partnered with local law enforcement agencies to give owners of at-risk vehicles free anti-theft devices. Hyundai is also offering free software upgrades to some of its vehicles that install better anti-theft protective measures. Source: Puget Sound Auto Theft Task Force & News Tribune

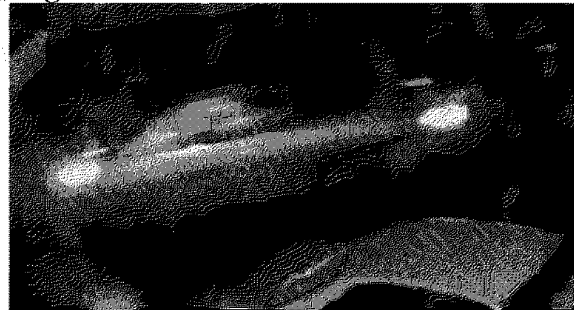
OFFICER SAFETY

	<h2>Special Bulletin</h2> <h3>TACOMA POLICE DEPARTMENT</h3>	
Bulletin Number: S23-058		Thursday April 20th, 2023
Detective A. McNeely #184 Tacoma Police Department Homicide / Aggravated Assault Unit Case Number: 23-099-00368		Office-(253) 830-6506 Cell-(253) 606-0820 jmcneely@cityoftacoma.org

Attempt to Identify Drive-by Shooting/Assault 1st – Vehicle



(Exact vehicle)



(Exact vehicle)



In the early morning hours of 4/9/23, a Drive-by Shooting occurred in the City of Tacoma, where the occupied residence of 1155 S 35th St was struck by one round fired from the street. The residence belongs to an elderly couple, who has lived at this location for several years. The round entered the residence through the closed front door and struck an elderly male, whom was sleeping in the front room, in the foot.

The believed suspect vehicle is captured on a neighbors surveillance cameras – which shows the above pictured sedan (believed to possibly be a 2 door 1990's Honda) passing by, and slowing down in front of, the residence multiple times. There is NO PC at this time, and this is an attempt to identify ONLY. The investigation remains ongoing.

The suspect(s) **HAVE NOT** been identified and are believed to be **ARMED AND DANGEROUS**.

If identified or any information please email or call Detective Aaron McNeely at 253-606-0820 or jmcneely@cityoftacoma.org.

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****

	<h2 style="margin: 0;">Special Bulletin</h2> <h3 style="margin: 0;">TACOMA POLICE DEPARTMENT</h3> <p style="margin: 0;">Bulletin Number: S23-057 Thursday April 20th, 2023</p>	
<p> Detective A. McNeely #184 Tacoma Police Department Homicide / Aggravated Assault Unit Case Number : 23-108-01383 </p>		<p> Office-(253) 830-6506 Cell-(253) 606-0820 jmcneely@cityoftacoma.org </p>

Attempt to Identify Drive-by Shooting/Assault 1st - Vehicle and Person of Interest



(Exact vehicle)





Person of Interest

On 4/18/23, a Drive-by Shooting occurred in the City of Tacoma, where the occupied residence of 7021 S Yakima Ave was struck approximately 10 times. The shooting is captured on a Ring Doorbell – across the street – which shows the above pictured station wagon (believed to possibly be a 1990's model Subaru wagon) firing the shots. Witnesses advise the shots are believed to come from the front right passenger side of the wagon. The Subaru abruptly stopped after driving away from the house, and the above shown male was seen exiting from the passenger side and getting onto a City bus heading W/B on S 72nd St. There is NO PC at this time, and this is an attempt to identify ONLY. The investigation remains ongoing.

The suspect(s) **HAVE NOT** been identified and are believed to be **ARMED AND DANGEROUS**.

If identified or any information please email or call Detective Aaron McNeely at 253-606-0820 or jmcneely@cityoftacoma.org.

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****

	TACOMA / PIERCE COUNTY REGIONAL INTELLIGENCE UNIT Intelligence Bulletin 23-02a Thursday, April 20, 2023	
Det. Sgt. John Delgado (253) 341-1369 john.delgado@piercecountywa.gov Gary L. Smith, Intel Analyst gary.smith@cityoftacoma.org (253) 594-7964		

****OFFICER SAFETY / SITUATIONAL AWARENESS****
(Update on Recent Activity on page2)



Jack, Alex James

DOB: 10/28/1995
W/M HGT: 5'5" **WGT:** 130lbs **Eyes:** Blue **Hair:**
Brown (last booking photo he had blonde hair, but is
naturally brown)
 (Tattoo on left side of neck that says "Loyalty")

LKA: Alex Jack has been living in a Silver BMW outside of the 1 Sector Substation, (1524 Martin Luther King Jr Way Tacoma WA 98405), since approximately January, WA Plate #CGY9107. He parks it on South 16th Street, just west of MLK. (Transient)

On 03/26/2023, at 1737 hours a Tacoma Police Officer at TPD HQ was informed that a male was outside the TPD building pointing around what looked like to be a handgun.); ALSO, WAS ACTING AS IF HE WAS GOING TO KICK IN A DOOR BUT HADN'T TOUCHED A DOOR YET. (JACK has a history of this at other government buildings).

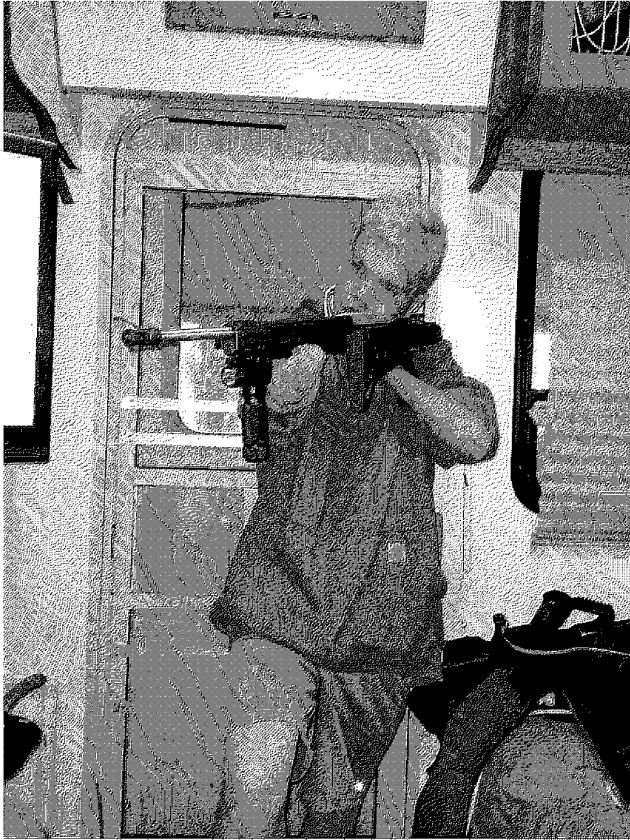
Last year in Fife he showed up to city hall and will yell, ramble and has done karate moves in the hallway of city hall and outside of the building. JACK was carrying around what looked like a red hose attachment, while pointing it around as if it was a gun. The TPD Officers stepped outside HQ as he dropped the red attachment onto the ground. JACK informed officers that he was just "trying to impress SWAT".

JACK has mental health issues and has a history of carrying extremely realistic looking BB and pellet guns. Officers had walked to the Honda he was driving and observed what appeared to be an AR-15 style BB gun in the back seat, which Jack later confirmed was just a BB gun". Even though JACK's arms are cut off around the elbow he is able to manipulate the guns. JACK is fixated on police and the stations. He has been contacted at multiple stations and other police departments.

*Alex Jack was last reported at the main entrance of City Hall in Tacoma and spent 3 hours in front of County Corrections on 4/7/2023. Jack has also frequented Puyallup City Hall in the past.

His behavior at the police stations were described as alarming and made people feel unsafe.

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****



Update Alex Jack continues to show an interest in Police Activities and LE Facilities! Recently on Social Media he has posted pictures of himself with real firearms. Previously has been seen with an AR-15 style BB/Pellet gun as mentioned before, however, the one in the picture below is a Ruger 10/22. *He has also posted "Was supposed to be the mass shooter".



***Law Enforcement Officers need to continue to be aware of his possible activity and any future contact with Alex J. JACK, they should handle with extreme caution and safety.**

If there any future incidents with JACK, report to the SSRIG at PCINTEL@piercecounitywa.gov



***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****

OFFICER AWARENESS

	<p style="text-align: center;">Patrol Information Bulletin <i>Bonney Lake Police Department</i></p> <p>Case # 2308801965</p> <p>Title: Vehicle Prowl/Fraud</p>	
<p>Prepared by: Detective T. Johnston johnstont@cobl.us</p>		<p><i>Bryan Jeter, Chief of Police</i> Jeterb@ci.bonney-lake.wa.us</p>

BOLO

Last seen in this vehicle, a reported stolen, 2015 Ford Flex, out of Pierce County. It should have a sticker in the right lower rear window of a bird's head



On March 29th, 2023, Smith associated with a maroon Ford Flex with no plates broke the window of the victim's vehicle in the Planet Fitness parking lot. The victim's wallet containing his ID and several credit cards were taken and later used at the Muckleshoot Casino.

Smith is a suspect in numerous cases throughout Pierce and King County where he prowls vehicles and then immediately uses the victim's credit card at casinos.

Austin L. Smith (09/23/1996)
Multiple No Bail Felony Warrants

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****



This bulletin is for information only, if you come into contact with Smith, please arrest him on his warrants and notify Bonney Lake Detective Johnston at 253-261-5793.

CYBER THREATS

A [Computer-Generated] Swatting Service Is Causing Havoc Across America

As the U.S. deals with a nationwide swatting wave, Motherboard has traced much of the activity to a particular swatting-as-a-service account on Telegram. Torswats uses synthesized voices to pressure law enforcement to specific locations. ... Motherboard's reporting on Torswats comes as something of a nationwide swatting trend spreads across the United States. In October, NPR reported that 182 schools in 28 states received fake threat calls. Torswats' use of a computer-generated voice also comes as the rise of artificial intelligence poses even greater risks to those who may face harassment online. In February, Motherboard reported that someone had doxed and harassed a series of voice actors by having an artificial intelligence program read out their home addresses. Source; VICE, 4/13/2023



Analyst Comment A Telegram channel is reportedly behind a months-long swatting campaign causing panic across the United States. A recent article published by Vice states that the hundreds of swattings called into high schools, businesses, and private residencies stem from the Telegram channel Torswats operating a swatting-for-service operation. According to the channel, users can purchase a computer-generated swatting call to a school for \$75. Additionally, a user can purchase an "extreme swatting" that will likely result in the victim being handcuffed by law enforcement for \$50. All payments are taken in cryptocurrency, and discounts are offered to returning users. The channel uploaded 35 recordings of their swatting calls. Each recording file is numbered. It is very likely that Torswat conducted more than the calls listed on its channel. The calls use a synthesized voice and switch between male and female voices. The campaign has called local emergency responders in Texas, Pennsylvania, Florida, Virginia, Maryland, Washington, California, and Texas, claiming a bomb threat or active shooting is occurring. Swatting can present a significant risk to both the victim and responding officers. In 2017, a swatting call resulted in the death of a 28-year-old Kansas man. The person responsible for the call, a serial swatter, is serving a 20-year sentence for the incident. Source; Surface Transportation & Public Transportation ISAC Transit & Rail Intelligence Awareness Daily Report (TRIAD)

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****



What it Will Look Like if China Launches Cyberattacks in the U.S.

While much of the cybersecurity world's attention is on fending off Russian hacks against Ukraine, American officials are increasingly worried about another growing threat: attacks by China on U.S. soil. If China invades Taiwan, they say, it is likely to unleash a volley of digital strikes against the United States at the same time. Beijing continues to issue bold threats against the island. Most recently, China renewed military drills around the island in response to last week's meetings in the U.S. between Taiwan's president and

House leaders — a meeting China called a “provocation.” Top lawmakers, the U.S. intelligence community and cybersecurity officials have warned in recent weeks that if an invasion happens, China would likely try to hobble critical U.S. systems with cyberattacks on military transport systems like ports and railroads, or against key civilian services like water and electricity. Source: Politico, 4/16/2023

Analyst Comment On 5 April, U.S. Speaker Kevin McCarthy and Taiwanese President Tsai Ingwen, alongside other bipartisan House lawmakers, met in Los Angeles, California. As a result of the meeting, Speaker McCarthy became the “highest U.S. official to meet with Taiwan’s leader on domestic soil since the U.S. established formal diplomatic ties with China in 1979.” In response, the People’s Republic of China called the meeting a “provocation,” threatened retaliation, and conducted a series of renewed military drills around Taiwan. The heightened tensions resulted in the U.S. intelligence community and U.S. lawmakers warning that if China invades Taiwan, “[China] is likely to unleash a volley of digital strikes against the United States at the same time,” particularly against critical infrastructure sectors. According to Representative Mike Gallagher, Chair of the House Select Committee on China, “If Xi Jinping moves on Taiwan, we should assume he’ll launch cyberattacks against the United States as part of the operation likely [including] attacks on our electrical grid, water systems and communications infrastructure — especially near key military installations.” The U.S. Intelligence Community’s annual threat assessment, released in February 2023, warns that “If Beijing feared that a major conflict with the United States were imminent, it almost certainly would consider undertaking aggressive cyber operations against U.S. homeland critical infrastructure and military assets worldwide,” and “such a strike would be designed to deter U.S. military action by impeding U.S. decision making, inducing societal panic and interfering with the deployment of U.S. forces.” Source: Surface Transportation & Public Transportation ISAC Transit & Rail Intelligence Awareness Daily Report (TRIAD)

PUBLIC SAFETY



(U) PREPARED BY THE FBI OFFICE OF PARTNER ENGAGEMENT
AND CRIMINAL INVESTIGATIVE DIVISION

11 APRIL 2023

[DPE-23-SA-010]

(U) Upward Trend in Telephonic Hoax Active Shooter Threats to US Education Institutions Nationwide in 2023

(U) SITUATIONAL AWARENESS

*** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY ***

(U//FOUO) From 1 January to 1 March 2023, elementary, secondary and higher education institutions in the United States observed an upward trend in telephonic hoax active shooter threats. Hoax threats – also known as swatting – have prompted law enforcement (LE) to swarm a location where an active shooting was reportedly in progress.¹ These hoax calls can be used as a tactic for an ambush if a person specifically calls with the intent to target respondents. Individuals making claims of high-risk situations, such as active shooter or other threats to life, not only misdirect LE resources from actual public safety needs, they also place the public in potential physical danger while creating a sense of fear or panic. Moreover, false reports can result in the public questioning the validity of future threats.

(U) In 2023, multiple states have experienced an upward trend in telephonic hoax active shooter threats including Arizona, California, Colorado, Florida, Georgia, Idaho, Kansas, Massachusetts, Michigan, Minnesota, Nevada, New Mexico, New York, Ohio, Oklahoma, Oregon, Texas, and Vermont. Several states reported multiple hoax threats during a single day – allowing local LE to identify the call source and quickly inform other local LE departments.

(U//FOUO) The FBI analyzed telephonic hoax active shooter incident reports from January to March 2023 and determined the threats contained variations in language, script, and other unique identifiers. In some reports, the caller claimed to be a victim trapped inside a school due to an active shooter incident. In other reports, the caller claimed they were outside an identified school and threatened to use firearms or bombs. The motivation for these hoax calls has not been determined.

(U) The purpose of this Situational Awareness report is to raise awareness of hoax active shooter calls made by unidentified callers targeting US education institutions. This threat is similar to those reported in the August 2022 Public Safety Awareness Report [OPE-22-SA-019], which evaluated over 187 telephonic hoax bomb threats to universities and colleges nationwide from 27 June to 5 August 2022.

(U) This awareness report is based on information obtained from incident reports and open source reporting. All active shooter threats should be taken seriously and actioned with appropriate security protocols.

(U) CONSIDERATIONS

(U//FOUO) Notable characteristics of the telephonic active shooter threats include, but are not limited to, any individual, group, or activity (these indicators should be observed in context and not individually):

- (U) The caller is male
- (U) The caller has a heavy foreign accent
- (U) The caller is using a VOIPa number, often tied to a service called TextNowb
- (U) The caller hacked or found other means to access digital infrastructure, providing a false location
- (U) The caller rapidly dials or re-dials indicating systematic targeting of institutions
- (U) The same caller conducts an influx of hoax calls during a discrete timeframe that impacts different LE areas of responsibility
- (U) Some calls ended with sounds of gunfire.

(U) RESOURCES

- (U) The FBI encourages our federal, state, local, tribal, and territorial (FSLTT) law enforcement partners and the public to report any suspicious activities and threats to the FBI's National Threat Operation Center by calling 1-800-CALL-FBI (225-5324), visiting <https://tips.fbi.gov/> or by contacting their local FBI Office: <https://www.fbi.gov/contact-us>.
- (U) We also encourage the law enforcement use of the unclassified information sharing system eGuardian for reporting suspicious activity reports (SARs) to the FBI. Access eGuardian via the Law Enforcement Enterprise Portal (LEEP): <https://www.cjis.gov/>.
-

Source: (U) PREPARED BY THE FBI OFFICE OF PARTNER ENGAGEMENT AND CRIMINAL INVESTIGATIVE DIVISION

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****

a (U) VOIP is a technology allowing a user to make voice calls using a broadband internet connection instead of a regular phone line.

b (U) In October 22, TextNow, one of many free or low-cost Internet-based calling platforms, blocked Ethiopia from its service and further restricted its service to North America; however, the calls have continued and extended into additional states, including Alaska, Maine, and Oregon. Source: Online newspaper article | NPR | "Federal authorities investigate a case about false threats of school shootings" | 28 November 2022 | <https://www.npr.org/2022/11/28/1139388765/federal-authorities-investigate-a-case-about-false-threats-of-school-shootings> | accessed on 5 December 2022.

NATIONAL

(U//FOUO) Transnational: New Eco-Extremist Publication Highlights Critical Infrastructure Vulnerabilities

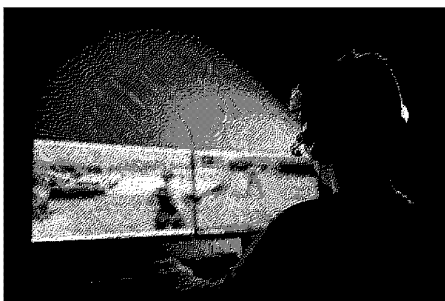


(U//FOUO) According to a New York City Police Department (NYPD), NYPD Intelligence and Counterterrorism Bureau (ICB) and NYPD Counterterrorism Division Daily Terrorism Brief dated 09 APR 23, open-source reporting indicated on 06 APR 23, the inaugural issue of a recently released, 43-page eco-extremist publication titled "Anti-Tech Quarterly...Freedom from Technological Slavery" (ATQ), outlined vulnerabilities associated with US and European critical infrastructure that can be exploited. The authors described the publication, which is dated 31 MAR 23, as a continuation of another eco-extremist magazine called "Garden." While the document claimed that its writers, "do not advocate that anyone consider this publication an exhortation for violent or illegal

action of any kind," the cover of the magazine and promotional hashtags branded it as a work of "Kaczynskism," referring to Ted Kaczynski—the so-called "Unabomber" who killed three and injured nearly two dozen in a series of improvised explosive device attacks from 1978 to 1995. The issue did not explicitly provide tactical guidance, but offered detailed explanations of the ways in which critical infrastructure systems are vulnerable.

For example, it noted that the electric utility industry has plans in place in case of a wide-scale grid failure and that, "these preparations do not guarantee the resiliency of the grid but reveal what the next steps for restoration would likely entail." Various online communities associated with eco-extremists and accelerationist extremists have reportedly shared the publication since its release.

(U//FOUO) NYPD / NYPD ICB / NYPD Counterterrorism Division Comment: The release of this latest magazine reflects Eco extremists' and accelerationist extremists' continued prioritization of critical infrastructure targeting. Additionally, the magazine provided a Protonmail email address and Instagram account for anyone interested in contributing to future issues, signaling that the publication likely features a collection of content from a number of authors; this is typical of similar documents circulating in online extremist communities. (NYPD / NYPD ICB / NYPD Counterterrorism Division, Daily Terrorism Brief, 09 APR 23)



(U) United States: Threat of Extremism in Online Video Game Communities

(U//FOUO) The Orange County Intelligence Assessment Center (OCIAAC) and the Federal Bureau of Investigation Los Angeles (FBI LA) provide this Joint Information Bulletin (JIB) to encourage law enforcement, particularly School Resource Officers (SROs), to increase awareness of the use of online gaming platforms to promote extremist ideologies through recruitment, propaganda, and threats. Online video games and related platforms provide opportunities for connecting with

*** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY ***

people both domestically and internationally, and the content of certain games may appeal to extremists. For example, games set during World War II may attract individuals with white supremacist ideologies, and multiplayer interactions could facilitate networking between such individuals.

Additionally, external communication platforms used in conjunction with online gaming can provide a private end-to-end encrypted environment for open and anonymous discussion with little to no negative consequences.

(U//FOUO) Online video games have become a prominent recreational activity worldwide, especially for children and teens. The subject matter of certain games, coupled with creative freedom, anonymity, online functionality, and relative privacy of communication, has made them attractive tools for extremists to propagate their beliefs and increase their sphere of influence. Furthermore, both video games themselves and chat programs associated with video gaming have been cited by successful mass attackers as a means by which they planned and practiced their attacks. Local to Orange County, several recent reports have cited threats with a gaming nexus:

- (U//FOUO) On 10 OCT 22, a reporting party received a threatening message with racist remarks via USBUS Discord (an encrypted messaging application common among gamers). The reporting party explained that he used to play online video games with the subject. In November 2022, the reporting party received additional threats from the subject and was the victim of a swatting call.
- (U//FOUO) On 12 APR 22, a subject posted references on social media to involuntary celibate (Incℓ) ideology. The subject further stated a desire to become a mass shooter and live stream the attack on USBUS Discord.
- (U//FOUO) On 14 JUN 21, Orange County law enforcement officers responded to a local middle school. According to school administration, three students used their school laptop computers to make threatening statements about killing students. The conversation identifies three usernames: "School Shooter," "Nathan," and "Cruz," likely referring to USPER Nikolas "Cruz," the Parkland, Florida school shooter. One student stated his idea of committing a school shooting came from a video game, but the game mentioned contains no references to school shootings.

(U) Activities and Indicators

(U//FOUO) Online gaming environments have been targeted recently by international hate groups, especially those comprised of juveniles and young adults, as a means to recruit members. These groups maintained external chat rooms where photos, information, and plans were shared, including death lists/threats, gore, and extreme violence, allegedly procured weapons, extremist ideology/memes, bomb-making instructions, and guidance for 3D printing weapon parts.

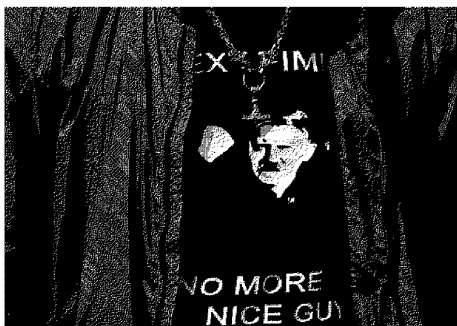
(U//FOUO) Indicators of extremism in gaming include:

- (U//FOUO) User created content emulating significant events supporting the ideology, reenactments of previous mass attacks,
- or simulations of violence/criminal acts;
- (U//FOUO) Hate speech or threats in chats, private messages, or usernames;
- (U//FOUO) Solicitations to participate in outside extremist ideology chats; and/or
- (U//FOUO) Manipulations of in-game environments to display or advertise extremist ideologies.

(U) Consideration and Reporting

(U//FOUO) The OCIAC encourages its partners, particularly SROs, to familiarize themselves with online gaming platforms and communication applications to be able to recognize indicators of radicalization. Hate speech can be common on video game platforms and therefore may not always be reported. Enforcement of anti-hate speech policies vary by platform. Maintaining awareness of groups, games/platforms/apps used, and key terms or images, may aid in identifying those at risk of being indoctrinated into extremism. (OCIAC / FBI LA, JIB, Threat of Extremism in Online Video Game Communities, 12 APR 23) Source: Army Threat Integration Center (ARTIC)

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****



DHS Warns U.S. Extremists Pose Growing Threat to Cops, Reporters, Pipelines

Domestic violent extremists from different parts of the political spectrum pose a growing threat to law enforcement, journalists and sites linked to the nation's critical infrastructure, according to U.S. intelligence obtained by Newsweek. The document, titled "Terrorist Media Trends: March 2023" and attributed to the Department of Homeland Security's (DHS) Office of Intelligence and Analysis highlighted risks from domestic extremists from both the left and right. Among its examples were protesters who attacked police in Atlanta last month as well as concerns over narratives justifying violence against

the LGBTQ+ community after the deadly March 27 shooting at a Christian school in Nashville by a shooter who identified as transgender. Coming at a time of growing political polarization in the U.S., the document warned that "online media produced by terrorist organizations and domestic violent extremists (DVEs) in March 2023 aimed to provide guidance for attacks against law enforcement, journalists, and soft targets using simple tactics." Source: Newsweek, 4/20/2023

Analyst Comment 14 April, the Department of Homeland Security (DHS) Office of Intelligence and Analysis (I&A) published a document titled "Terrorist Media Trends: March 2023," outlining changes to terrorist and Domestic Violent Extremist (DVE) justifications, tactics, targets, reach, and appeal that can be determined from terrorist/DVE media. According to the document, "online media produced by terrorist organizations and [DVEs] in March 2023 aimed to provide guidance for attacks against law enforcement, journalists, and soft targets using simple tactics." March also saw an increase in DVE rhetoric urging attacks against critical infrastructure, particularly against electrical substations and an oil pipeline in Alaska. According to Brian Harrell, former DHS Assistant Secretary for Infrastructure Protection, the document "simply acknowledges what industry has been monitoring for months now." Harrell added that the document's contents are "a growing trend here in the U.S., but also globally" and that "industry owns the infrastructure, so it's imperative that the private sector stay coordinated with law enforcement and National Security partners." The DHS document did not disclose any specific credible imminent threats to transit or transportation infrastructure. However, the potential for attacks cannot be ruled out entirely. Likewise, the proximity of transportation infrastructure to populated spaces, other critical infrastructures, and iconic locations allows for the possibility that transportation employees, patrons, and assets could also be impacted by violent or destructive acts that do not intentionally target the sector directly. Source: Surface Transportation & Public Transportation ISAC: Transit & Rail Intelligence Awareness Daily Report (TRIAD)

INTERNATIONAL



Some U.S. Cities May Offer Model to Ease Canada Transit Violence: Experts

As Canadian cities look for ways to combat violence on public transit, experts say strategies south of the border that combine law enforcement, social supports and community engagement could offer new solutions. Violence on transit has captured national attention in recent weeks — a 17-year-old boy was fatally stabbed on a Vancouver-area bus last week, a man had life-threatening injuries after his throat was slashed on a Surrey, B.C., bus earlier this month, and a 16-year-old boy was stabbed to death in an unprovoked attack at a Toronto subway station in March. Those high-profile cases were among many other instances of aggression on transit in

several cities. Transit agencies and police have been working to understand what's driving the violence, with some pointing to the pandemic as a factor. Social issues including housing and mental health converged on public transit in recent years because that was one of the few public spaces that remained open during the COVID-19 pandemic. Source: National Post, 4/19/2023

*** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY ***

Analyst Comment Violence on Canadian transit systems has been the subject of nationwide attention recently after a series of stabbings on buses and in transit stations were perpetrated over the past few weeks. According to a report released by the Toronto Transit Commission (TTC) on 13 April, offenses committed against TTC customers spiked from December 2022 to January 2023, reaching a record high of 2.72 offenses per million customers in January, which is approximately three times higher than the number of offenses against customers the transit agency saw from 2017 to 2019. The spike seen in January prompted the TTC to take a “multidisciplinary approach” to reduce crime, which involved the introduction of Community Safety Ambassadors, increased Special Constables and security personnel in transit stations, increased police presence and patrols, and the promotions of the SafeTTC app and “See Something Say Something” campaigns. In February, offenses against TTC customers were down 18% from their high in January, and the reduction is attributed to the new safety measures. Going forward, the TTC plans on hiring 55 additional Special Constables, nine of which will be hired this month. In the U.S., many transit organizations have taken multipronged approaches to reducing transit violence by addressing mental health, substance abuse, and housing issues in addition to increasing security personnel. Source: Surface Transportation & Public Transportation ISAC Transit & Rail Intelligence Awareness Daily Report (TRIAD)



United States: (UPDATE) Justice Department Arrest Chinese Nationals Citing “Secret Police Station”

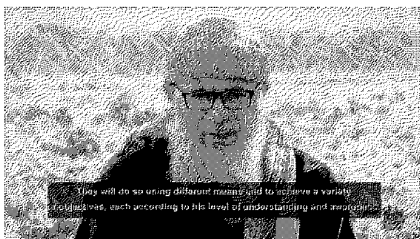
Two men were arrested Monday on charges that they helped establish a secret police station in New York City on behalf of the Chinese government, and about three dozen officers with China’s national police force were charged with using social media to harass dissidents inside the United States, authorities said Monday. The cases are part of a series of Justice Department prosecutions in recent years aimed at disrupting Chinese government efforts to locate in America pro-democracy activists and others who are openly critical of Beijing’s policies and to suppress their speech. One of three cases announced Monday concerns a local

branch of the Chinese Ministry of Public Security that had operated inside an office building in Manhattan’s Chinatown neighborhood before closing last fall amid an FBI investigation.

The two men who were arrested were acting under the direction and control of a Chinese government official and deleted communication with that official from their phones after learning of the FBI’s probe in an apparent effort to obstruct the inquiry, according to the Justice Department. The Justice Department’s arrest follows several similar investigations across the United Kingdom and Europe. In addition, prosecutors on Monday announced that eight Chinese government officials who are believed to be currently living in China were charged with directing an employee of a U.S. telecommunications company to remove Chinese dissidents from the company’s platform. Source: Justice Department, PBS Newshour, Politico Europe

Analyst Note Law Enforcement officials charged 34 Chinese security officers with operating a transnational repression scheme aimed at Chinese nationals living in the U.S. Two men were arrested in NYC for operating an unofficial police station, used to locate pro-democracy activists and pass that information to security officials in China. The 2024 Presidential elections are approaching with warnings from U.S. intelligence and law enforcement agencies of increased foreign malign information campaigns directed to sow discord and interfere in or influence elections. A report by DOJ and DHS reviewing foreign interference found broad campaigns by government-affiliated actors (primarily from Russia, China, and Iran) targeting infrastructure, undermining public confidence in election infrastructure, using social media platforms to spread propaganda and mis/mal/dis-information, and attempting to infiltrate U.S. political organizations. The report recommended a hardening of physical and cyber security of the election infrastructure, increased public messaging to provide timely and accurate information, and engagement and cooperation between federal, state, local and private-sector partners to safeguard the next election from foreign interference. Source: Watchline@fdny.nyc.gov

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****



U.S. Adds Al Qaeda Leader in Syria to List of Global Terrorists

The U.S. State Department added Sami al-Uraydi, a senior leader of Al Qaeda's branch in Syria, to its list of Specially Designated Global Terrorists. State's Rewards for Justice program previously offered a \$5 million bounty for information leading to the arrest and prosecution of al-Uraydi. State offered little other information on al-Uraydi in yesterday's

designation, only noting he was being designated as a result of his senior leadership position in HAD. Al-Uraydi, who is also known by his kunya as Abu Mahmud al-Shami, was previously identified by State, however, as "a Jordanian national and senior sharia official for Hurras al-Din" (HAD, or the "Guardians of Religion organization)." Al-Uraydi is a known al-Qaeda loyalist who was closely allied with former al-Qaeda emir Ayman al Zawahriri. Source; Long War Journal, 4/13/2023

Analyst Comment On 12 April, the U.S. Department of State added senior Al Qaeda leader in Syria Sami al-Uraydi to its Specially Designated Global Terrorists list. Sami al-Uraydi, who is also known as Abu Mahmud al-Shami, was previously identified by the Department of State as "a Jordanian national and senior sharia official for Hurras al-Din" (HAD), which translates to "Guardians of Religion Organization." The HAD formed in 2018 as a splinter organization from the former Al NusraFront and is now assessed to be Al Qaeda's official branch in Syria. The HAD has an estimated 2,000 to 2,500 members and is most prominent in the Idlib region of Syria, near the Turkish border, according to the U.S. Office of the Director of National Intelligence (ODNI). The U.S. Department of State said that HAD engages in "killings, kidnappings, and violence targeting of members of religious minority groups" and offered a \$5 million reward for information leading to the capture of al-Uraydi. According to the U.S. government, in addition to his participation as a leadership element within the HAD, al-Uraydi has also historically been "involved in terrorist plots against the United States and Israel." Source; Surface Transportation & Public Transportation ISAC Transit & Rail Intelligence Awareness Daily Report (TRIAD)

Other National/International Articles of Interest (Links):

United States: At Least 193 Suspected of Being Involved in Terrorism Have Crossed the Southern Border

<https://thehill.com/opinion/immigration/3959839-at-least-193-suspected-of-being-involved-in-terrorism-have-crossed-the-southern-border/>

'Abominable' MS-13 leader 'Indio de Hollywood' under arrest and facing terrorism, RICO charges: Feds

<https://lawandcrime.com/crime/abominable-ms-13-leader-indio-de-hollywood-under-arrest-and-facing-terrorism-rico-charges-feds/>

United States/Sudan: Pentagon Prepping for Potential Evacuation of US Embassy Staff from Sudan

<https://thehill.com/policy/defense/3961129-pentagon-prepping-for-potential-evacuation-of-us-embassy-staff-from-sudan/>

The changing landscape of electric vehicle adoption in law enforcement

https://www.police1.com/police-products/vehicles/patrol/articles/the-changing-landscape-of-electric-vehicle-adoption-in-law-enforcement-GDDvga7tXsmKGDhy/?utm_source=Police1&utm_campaign=9fa65f3dc5-EMAIL_CAMPAIGN_2023_04_17_06_28&utm_medium=email&utm_term=0_5584e6920b-9fa65f3dc5-%5BLIST_EMAIL_ID%5D

*** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY ***

Neo-Nazi Fight Clubs Are Fat-Shaming Men into White Nationalism

<https://www.vice.com/en/article/n7evgw/neo-nazi-fight-clubs-robert-rundo-fat-shaming-white-nationalism>

2 Chinese nationals charged with operating a secret police station in NYC

<https://www.nbcnews.com/news/2-chinese-nationals-charged-operating-secret-police-station-new-york-c-rcna80076>

Tackling imposter syndrome mentality

[https://www.police1.com/health-wellness/articles/tackling-imposter-syndrome-mentality-Lx6qpUOrvMjbNVIE/?utm_source=Police1&utm_campaign=9fa65f3dc5-](https://www.police1.com/health-wellness/articles/tackling-imposter-syndrome-mentality-Lx6qpUOrvMjbNVIE/?utm_source=Police1&utm_campaign=9fa65f3dc5-EMAIL_CAMPAIGN_2023_04_17_06_28&utm_medium=email&utm_term=0_5584e6920b-9fa65f3dc5-%5BLIST_EMAIL_ID%5D)

[EMAIL_CAMPAIGN_2023_04_17_06_28&utm_medium=email&utm_term=0_5584e6920b-9fa65f3dc5-%5BLIST_EMAIL_ID%5D](https://www.police1.com/health-wellness/articles/tackling-imposter-syndrome-mentality-Lx6qpUOrvMjbNVIE/?utm_source=Police1&utm_campaign=9fa65f3dc5-EMAIL_CAMPAIGN_2023_04_17_06_28&utm_medium=email&utm_term=0_5584e6920b-9fa65f3dc5-%5BLIST_EMAIL_ID%5D)

Instagram scam promises money in exchange for your image

https://www.malwarebytes.com/blog/news/2023/04/instagram-scam-promises-money-in-exchange-for-your-image?&web_view=true

‘Where’s the Livestream?’: Louisville Shooting Reactions Show Growing Role of Videos in Extremist Messaging

<https://www.hstoday.us/featured/wheres-the-livestream-louisville-shooting-reactions-show-videos-growing-role-in-extremist-messaging/>

An Oklahoma City bombing survivor on why he’s worried about extremism today

<https://www.pbs.org/newshour/nation/watch-an-oklahoma-city-bombing-survivor-on-why-hes-worried-about-extremism-today>

*TPD/PCSD Homeland Security Reports Received this week 8.

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****

To: SHRCOMMISSIONED[SHRCOMMISSIONED@piercecounitywa.gov]; SHRJCO[SHRJCO@piercecounitywa.gov]
Cc: David Hutchinson[david.hutchinson@piercecounitywa.gov]
From: Gary Smith
Sent: Fri 4/28/2023 2:55:26 PM
Subject: SSRIG Weekly Intelligence Summary 17 - 2023 (April 28, 2023)
Received: Fri 4/28/2023 2:55:37 PM
[SSRIG Weekly Summary 17-2023.pdf](#)

South Sound Regional Intelligence Group SSRIG email: PCINTEL@piercecounitywa.gov Weekly Summary	
#17-2023	April 28, 2023
Gary Smith Intelligence Analyst Gary.Smith@ci.tacoma.wa.us (253) 594-7964	
This document is a FOUO communication and is not to be disseminated outside of the law enforcement or intelligence communities. Dissemination to media sources is not authorized.	

REGIONAL

(U//FOUO) United States: Online Sharing of Tactics from Firearms Attacks Increases Threat to US Electrical Infrastructure

(U//LES) Demand for Synthetic Opioid Nitazene in Spokane, Washington, as of late 2022

(U//FOUO) Online Child Exploitation Group 764 Encourages Victim Self-Mutilation and Suicide

OFFICER SAFETY

(U) Bandidos Motorcycle Club Members Expected to Travel to Washington State to Attend Memorial Service on 29 April 2023

OFFICER AWARENESS

PC to Arrest- Drive-By Shooting; TPD Case # 2310101748

OFFICER SAFETY CONCERN – HOMICIDE SUSPECT

ATTEMPT TO IDENTIFY-ARMED ROBBERY SUSPECTS

Theft/Fraud Suspect Traveling in Washington

Information: Eluding and Street Racing Suspect

CYBER THREATS

(U) Cyber: New Credential-Stealing Malware Advertised on Telegram

(U//FOUO) Cyber: Criminals Exploit Online Marketplaces to Engage in Carjackings and Resale of Stolen Vehicles

PUBLIC SAFETY

FBI: Active Shooter Incidents Fell in 2022 but Remained Relatively High

NATIONAL

(U//FOUO) United States: Juveniles Will Likely Leverage Explosives Availability to Target Secondary Schools

Pitt Researchers Collect Data on Where Train Accidents Occur and What They Threaten

INTERNATIONAL


Germany Arrests 28-Year-Old Syrian Over 'Radical Islamist' Bomb Plot

Sudan in Chaos



Other National/International Articles of Interest (Links):

Gary L. Smith

Gary L. Smith
Criminal Intelligence Analyst
Regional Intelligence Group
TPD/PCSD
Tacoma, WA
(253) 594-7964
(253) 405-6214 (C)
gary.smith@cityoftacoma.org
gary.smith@piercecounitywa.gov

"There must be a Lone Ranger!" 

*** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY ***

	<p>TACOMA / PIERCE COUNTY REGIONAL INTELLIGENCE UNIT</p> <p>WEEKLY SUMMARY</p> <p>17-2023 Friday, April 28, 2023</p>	
<p>Det. Sgt. John Delgado (253) 341-1369 john.delgado@pierccountywa.gov</p> <p>Gary L. Smith, Intel Analyst gary.smith@cityoftacoma.org (253) 594-7964</p>		
<p>***** SENSITIVITY NOTICE *****</p> <p>This document is intended exclusively for the individual or entity to which it is addressed. This communication may contain information that is law enforcement sensitive, proprietary, privileged, confidential and may be legally protected or otherwise exempt from disclosure. If you are not the intended recipient, you are hereby notified that any disclosure, dissemination, copying or distribution of this transmission is strictly prohibited. If you have received this message in error, please notify the sender immediately by email and delete all copies of this message.</p> <p>**The SSRIG is a member of the Joint Terrorism Task Force. Agencies in Pierce County are encouraged to forward information first to The SSRIG and we'll be sure to forward the information accordingly.</p> <p>Please treat this and all other communications from this Regional Intelligence Unit as LAW ENFORCEMENT SENSITIVE. Further distribution of this document is restricted to law enforcement agencies, intelligence agencies, and Department of Defense organizations only, unless prior approval of this office has been obtained.</p> <p>THIS DOCUMENT OR ANY SEGMENT THEREOF, MAY NOT BE RELEASED TO ANY MEDIA SOURCES.</p> <p>*****</p>		

REGIONAL



(U//FOUO) United States: Online Sharing of Tactics from Firearms Attacks Increases Threat to US Electrical Infrastructure

Violent extremists are increasingly sharing tactics for attacking power stations, DHS Warns

(U//FOUO) According to a US Department of Homeland Security Office of Intelligence and Analysis (DHS I&A) Counterterrorism Mission Center Intelligence In Focus (IIF) dated 24 APR 23, in the past year, domestic violent extremists (DVEs) and other potential criminal actors have increased sharing of tactics from several firearms attacks against electrical power stations, likely escalating the threat to electrical infrastructure in the United States. Following a series of publicized, unrelated firearms attacks against electrical infrastructure over the past year, DVEs have increasingly circulated online messaging and operational guidance promoting attacks against this sector. The perpetrators of the attacks targeted electrical substations and transformers using tactics that can challenge law enforcement's ability to identify suspects and that have the potential to cause at least localized power disruptions.

- (U) Unidentified threat actors used firearms in several recent attacks against electrical infrastructure in the United States with varied success in destroying components critical to maintaining localized service. In December 2022, an unidentified perpetrator shot two substations in Moore County, North Carolina, causing power outages spanning several days and straining a wide range of businesses and healthcare, emergency, and other community services, according to media reporting.

- (U//FOUO) Over the past year, DVEs have shared best practices for firearms attacks against electrical infrastructure, including detailed diagrams, simplified tips for enhancing operational security, and procedures for disabling key components of substations and transformers, according to DHS and media reporting. The tactics used in recent firearms

*** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY ***

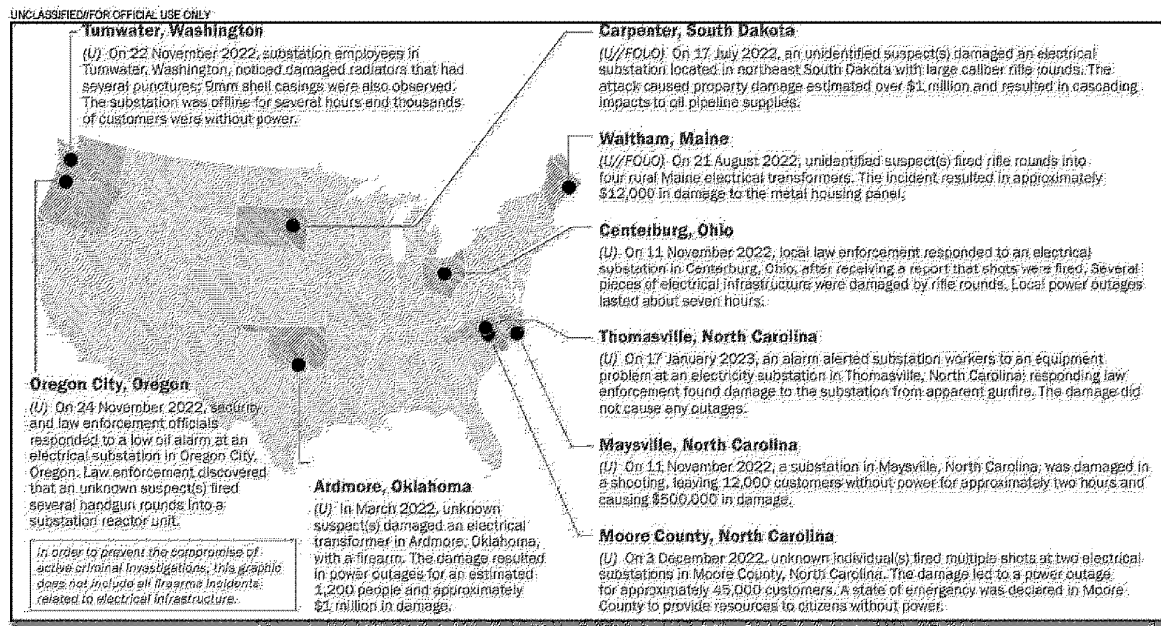
attacks are generally consistent with this guidance and have prevented law enforcement from identifying any of the perpetrators.

- **(U//FOUO)** DVEs and other criminal actors have referenced media coverage of the attacks, noting that they demonstrate proof-of-concept and are the best examples of successful attacks over the past decade, according to DHS and media reporting. Two racially and ethnically motivated violent extremists in Maryland referenced the North Carolina attack and were using publicly available information to identify substations for an attack before the plot was disrupted by law enforcement in February, according to a federal criminal complaint.

(U//FOUO) Firearms attacks could become more appealing and spread to other infrastructure sectors because they offer a low-risk/high-reward opportunity, other sectors feature similar vulnerabilities, and damage to electricity subsector targets could have cascading effects on other sectors. For example, similar tactics could be used to attack transportation and telecommunications targets if threat actors perceive these targets as sharing similar vulnerabilities, such as remote locales and a lack of onsite security personnel or other perimeter security measures. Threat actors also may target electrical infrastructure to indirectly disrupt operations they perceive as harmful to the environment or vital to law enforcement's ability to respond to criminal activity.

- **(U//FOUO)** Easily accessible rural infrastructure assets—such as pipeline systems, energy substations, and cell towers—are typically lightly guarded with cameras and simple physical barriers like fences and gates, making them vulnerable to low-risk firearms attacks that result in significant disruptions. Attacks on platforms in rural areas are harder to investigate, given the lack of witnesses and a longer police response time, judging from media and private sector reporting. Violent extremist media highlighting other vulnerable infrastructure could motivate offenders to target other less traditional critical infrastructure sectors.

- **(U//FOUO)** Blackouts caused by attacks on electrical infrastructure have the potential to cause strain or disrupt other critical infrastructure sectors, including communications; water and wastewater; public health; transportation; healthcare; and nuclear reactors, materials, and waste. In July 2022, components of an electrical substation in South Dakota were targeted by high-caliber rifle rounds, causing power outages and cascading disruptions to the Keystone Pipeline, according to government officials.



(U) Image of Selected Firearms Attacks on Electrical Critical Infrastructure Since March 2022

*** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY ***

(U//FOUO) Targeting Electrical Infrastructure Appeals to Various Domestic Violent Extremist Ideologies

(U//FOUO) Racially or ethnically motivated violent extremist messaging promoting narratives about accelerating societal collapse and encouraging a race war in support of accelerationist ideology has offered the most detailed instructions for firearms attacks against electrical infrastructure, though motives for attacks over the past year likely include various ideological and other motivations. Other DVE ideologies may share views that attacking electrical critical infrastructure is an effort toward achieving societal collapse. For example, involuntary celibate violent extremists have celebrated recent attacks on electrical infrastructure and encouraged additional attacks to “cripple the lifestyles” of the US populace, according to DHS reporting. (DHS I&A Counterterrorism Mission Center, Product Number: DHS-IA-IF-2023-08320, 24 APR 23)

Analyst Comment Following multiple high-profile attacks on US power substations last year, extremists have stepped up sharing of “online messaging and operational guidance promoting attacks against this sector,” says the DHS bulletin, which was distributed to US critical infrastructure operators on Monday. The information and tactics shared by extremists online include “detailed diagrams, simplified tips for enhancing operational security, and procedures for disabling key components of substations and transformers,” DHS warned. The last year saw a flurry of physical attacks and vandalism on US electric infrastructure. Tens of thousands of people lost power in Moore County, North Carolina, in December after Duke Energy substations were damaged by gunfire. On Christmas, thousands of people lost power in Pierce County Washington after someone vandalized multiple substations there. Source; DHS



**SITUATIONAL INFORMATION REPORT
FEDERAL BUREAU OF INVESTIGATION**

(Potential Activity Alert)

SEATTLE DIVISION

Approved for Release: 20 April 2023

SIR Number: SIR-00353349742

**(U//LES) Demand for Synthetic Opioid Nitazene in Spokane,
Washington, as of late 2022**

SOURCE: (U) An FBI Agent.

(U//LES) FBI Seattle is releasing this Situational Information Report to raise awareness amongst law enforcement and public safety officials regarding the possible appearance of the synthetic opioid nitazene in Spokane, Washington, as of late 2022. (Analyst comment: "Nitazene" describes a group of powerful illicit synthetic opioids linked to overdose deaths in several states. Until recently, the drug had been seen primarily in the midwestern, southern, and eastern United States.)

(U//LES) As of late 2022, FBI Seattle received reporting indicating demand for nitazene in the Spokane area. According to the reporting, drug users requested nitazene due to its potency, which was allegedly "twenty times" stronger than powdered fentanyl. In September 2022, suppliers planned to bring nitazene into the Spokane area.

(U//LES) As of April 2023, FBI Seattle did not possess any other information regarding the use or sale of nitazene in Spokane.

(U) This report has been prepared by the SEATTLE Division of the FBI. Comments and queries may be addressed to the SEATTLE Division at 206-622-0460. Source; Via Washington State Fusion Center

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****



**SITUATIONAL INFORMATION REPORT FEDERAL BUREAU OF
INVESTIGATION
(Activity Alert)
SEATTLE DIVISION**

Approved for Release: 24 September 2022 SIR Number: SIR-00350036819

**(U//FOUO) Online Child Exploitation Group 764 Encourages Victim
Self-Mutilation and Suicide**

SOURCE A: (U) A write-in to this agency. SOURCE B: (U) An employee of the FBI.
SOURCE C: (U) An officer of another law enforcement agency.

(U//FOUO) Online child exploitation group 764, also known as 764CVLT, targets vulnerable minors and coerces them to self-harm, produce child sex abuse material (CSAM), commit acts of animal cruelty, and live-stream their deaths by suicide via social media platforms. Victims who do not comply face retribution in the forms of extortion, doxing,[1] feeding,[2] and swatting.[3] Online groups KasKar, AAST, Legion, 7997, and Maniac Murder Cult (MYK) are offshoots of or affiliated with 764.

(U//FOUO) 764 members distribute the coerced content in online groups across social media platforms including Discord, Telegram, and Signal. 764 subjects identify and groom victims found on online videogames that offer chat functionality, including AmongUs and Roblox, as well as social media applications such as Instagram, Snapchat, Omegle, and Discord. Online mental health forums also provide opportunities for 764 members to identify highly vulnerable minors. Cutting serves as a physical identifier of potential 764 involvement. 764 members pressure victims into cutting "fan signs" or symbols into their bodies. These fan signs can include the subject's username or initials, "764," "cvlt," or white supremacist symbols such as swastikas.

(U//FOUO) 764 subjects target LGBTQ+ youth, racial minority youth, and minors who struggle with mental health issues to include depression, eating disorders, and suicidal ideation. Investigations into this group are complicated by the fact that many victims and subjects of 764 appear to be minors, with some subjects as young as 13 and victims as young as 12. 764's primary goal appears to be to coerce victims into producing more gore and/or explicit material, or to live-stream their deaths by suicide, rather than financial extortion. However, financial extortion has occurred in small amounts on some occasions.

[1] **ANALYST NOTE:** Doxing is defined as searching for and publishing private or identifying information about a particular individual on the internet, typically with malicious intent.

[2] **ANALYST NOTE:** Feeding is defined as the action or practice of writing or calling into a federal agency with the intent of federal law enforcement making contact with a target victim. This is similar to swatting, but with federal agents showing up to the victim's residence rather than a SWAT team.

[3] **ANALYST NOTE:** Swatting is defined as the action or practice of making a prank call to emergency services in an attempt to bring about the dispatch of a large number of armed police officers to a particular address. 764 members are known to swat victims as well as each other.

(U) This report has been prepared by the SEATTLE Division of the FBI. Comments and queries may be addressed to the SEATTLE Division at 206-622-0460. Source; Via Washington State Fusion Center

(U) **Warning:** This is an information report, not finally evaluated intelligence. It is being shared for informational purposes but has not been fully evaluated, integrated with other information, interpreted or analyzed. Receiving agencies are requested not to take action based on this raw reporting without prior coordination with the FBI.

(U) *Note. This product reflects the views of the SEATTLE Division.*

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****

OFFICER SAFETY

Upcoming OMG Activity



**SITUATIONAL INFORMATION REPORT
FEDERAL BUREAU OF INVESTIGATION
(Potential Activity Alert)
SEATTLE DIVISION**

Approved for Release: 26 April 2023
SIR Number: SIR-00353445402

**(U) Bandidos Motorcycle Club Members Expected to Travel to
Washington State to Attend Memorial Service on 29 April 2023**

SOURCE A: (U) An officer of another law enforcement agency.

SOURCE B: (U) An officer of another law enforcement agency.

(U//LES) The purpose of this Situational Information Report (SIR) is to raise awareness among law enforcement personnel and public safety officials regarding an expected increased presence of Bandidos Motorcycle Club members (Bandidos) traveling to Sedro Woolley, Washington in late April 2023 in order to attend a memorial service. The Bandidos MC is an identified "one-percenter," outlaw motorcycle gang (OMG).

(U//FOUO) A memorial service for Bryan Denson (Denson), the Bandidos Chapter President for Skagit County, is scheduled for 1pm on 29 April 2023 at Sunrise Christian Center, located at 10217 Collins Road, Sedro Woolley, Washington 98284. Denson passed away following a motorcycle accident in Mount Vernon, Washington on 18 March 2023. An estimated 250 people are expected to attend the service.

(U//FOUO) Reporting indicates Bandidos members plan to gather at a gas station on Bow Hill Road in Skagit County, Washington prior to the service and ride to the Sunrise Christian Center as a group. Members plan to meet at an unknown location following the service.

ANALYST NOTE: The referenced gas station is believed to be The Skagit Bow Hill Gas & Food Mart, located at 18520 Bow Hill Road, Bow, Washington 98232 (NFI).

(U//FOUO) **ANALYST NOTE:** Due to multiple upcoming funerals for Bandidos members in Texas, the number of out of state Bandidos traveling to Washington State for this memorial service may be limited.

(U//FOUO) FBI Seattle possesses no information regarding specific threats or planned acts of violence during these events. However, similar events involving Bandidos chapters have been associated with the potential for violence.



(U//FOUO) This report is for situational awareness for law enforcement personnel. Details of the event remain fluid. Recipients are requested to contact FBI Seattle if any positive information is developed regarding suspicious activity or potential violence by OMGs in Washington State.

(U) This report has been prepared by the SEATTLE Division of the FBI. Comments and queries may be addressed to the SEATTLE Division at 206-622-0460. Source; Via Washington State Fusion Center



*** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY ***

OFFICER AWARENESS

	<h1>Special Bulletin</h1> <h2>TACOMA POLICE DEPARTMENT</h2> <p>Bulletin Number: S23-060</p> <p>April 28, 2023</p>	
<p>Det. R. Beck Desk: 253-591-5679 Cell: 253-278-7020</p> <p style="text-align: right;">RBeck@CityofTacoma.org</p>		

PC to Arrest- Drive-By Shooting TPD Case # 2310101748



Vehicle from 4/11/23



DOL



BWC on 4/25/23

Cota Castro, Jose Angel
09/17/91
I/M, 511, 205 long Black hair,
unshaven

Associated Vehicle:
Green 2004 Chevy Tahoe WA-
CBR5004

Address: 2317 S 96th Street
BLDG C #315 (Terra heights)
Tacoma,

On 04/11/23, Cota-Castro was involved in a road rage incident in the area of S. 38th and Tacoma Avenue. As a result Cota-Castro pointed and shot a single round at another driver. The incident was recorded on dash-cam from the victim vehicle.

Cota-Castro uses multiple variations of his last name to include: Cota, Castro and Ancheta.

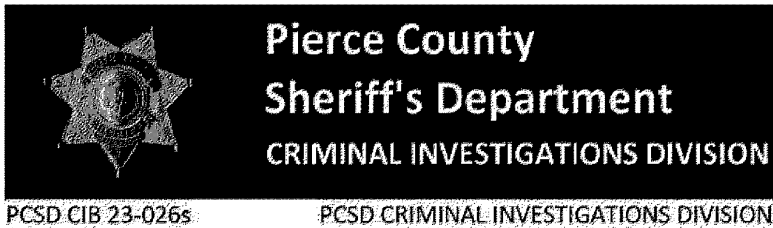
The listed vehicle is not registered to Cota-Castro but was parked at the address as recent as 04/25/23.

The firearm used in the incident and vehicle have not been recovered. Please use appropriate caution if contacting Cota-Castro as he has history of Assault 3, Eluding and listed "Highly Violent" through DOC.

If located please Notify Det. Beck by phone for an interview. The vehicle should be impounded for a search warrant and transported to TPD. Probable Cause exists to arrest and book Cota-Castro under the listed case number for Drive-by Shooting.

Det. Beck 253-278-7020 RBeck@CityofTacoma.org

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****



SPECIAL BULLETIN

April 27, 2023

OFFICER SAFETY CONCERN – HOMICIDE SUSPECT

The Pierce County Sheriff's Department is advising law enforcement to use caution with regard to the pictured vehicle, and any associated occupants. Manuele Samaga, is currently being investigated as a third suspect in a Homicide (PCSD Case #23-028-01706).

There is NO PROBABLE CAUSE yet for Manuele Samaga. Samaga has access to firearms. The other two suspects have already been arrested. It is likely Samaga knows or believes he is being investigated by law enforcement, so use extreme caution.

Do not stop, arrest or detain based on this bulletin. If this vehicle or any of the persons pictured below are contacted, use caution, as the firearm in this case has not been recovered.

Do not question Samaga or mention this case if he is stopped. Contact Detective Jacob Lawrence 253-377-5356 jacob.lawrence@piercecounitywa.gov, if you have any contact with Manuele Samaga.



NAME: Manuele I Samaga

DOB: 06/30/2004

PHY: 5'06" / 235 / BRO

LKA: 19002 96th Ave Ct E, Puyallup WA

VEH: Black 2013 Hyundai Accent WA License BJZ7126 (photo of Vehicle Below)



***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****

April 27, 2023,

ATTEMPT TO IDENTIFY-ARMED ROBBERY SUSPECTS

Pierce County Sheriff's detectives are attempting to identify the suspects responsible for an ARMED ROBBERY under PCSD Case #23-114-01725.

On April 25th, at 1637 hours, a 12-year-old boy was robbed at gun point of his silver necklace. The juvenile was walking home from school in the 178th block of 19th Ave E. when a gray pick-up truck possibly a Toyota Tacoma passed him then made a U-turn and came back and stopped. A Hispanic male in his 20s exited the passenger's side of the truck, pointed a black handgun at the victim and demanded the victim's silver chain necklace. After receiving the necklace, the suspect struck the victim in the face with the gun before getting back into the truck and fleeing. The victim said there were two older males in the truck.

SUSPECTS: Hispanic male mid-twenties 5'9" med with a buzz-cut. Suspects 2 and 3 were only described as older males.



If you have any information on the identity of this suspect, the vehicle or similar incidents, please contact Detective D. Moss Sr. at 253 798-7721 or darren.moss@piercesheriffwa.gov.

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****



SHERIFF

WASHINGTON COUNTY

ATTEMPT TO ID / BOLO

Case 50-23-5371
Deputy Tom Brown

Document prepared by WCSO for official use only and not to be disseminated without proper permission. The information contained herein does not establish or convey authority to arrest, stop, detain, or tow, unless specifically stated. For questions, contact WCSO Investigations at (509) 846-2500.

Theft/Fraud Suspect Traveling in Washington



On 04/11/2023, the pictured suspect used stolen credit cards to buy numerous expensive items at the Apple Store in Tigard OR (7273 SW Bridgeport Rd). The cards had been in a wallet stolen at St Vincent Hospital in Portland.

Please be on the lookout for this suspect and the pictured vehicle, which he was traveling in at the Apple Store. If your agency has any related cases or helpful information, please contact WCSO Deputy Tom Brown.

FURTHER INFO: On the day of the crime, an Apple AirTag in the stolen wallet transmitted northward on I-5 in Washington State. It stopped at several locations (including Emerald Queen Casino at 2920 East R St in Tacoma) on the same day, en route to the Seattle area.

The AirTag continues to transmit near Pacific Medical Center (1200 12th Ave S) in Seattle from 0700- 1500 hrs on Monday-Friday. And overnight, the device's signal is consistently near 11215 26th Ave S in Burien, where the AirTag appears to be left in a parked vehicle. **We're currently contacting agencies in those areas, but if you have any helpful information, don't wait for us to reach out! Please use the email link above.

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****



KENT POLICE DEPARTMENT

BULLETIN# 23-18 UPDATE

Published by: Commander J. Bava

E-mail: jbava@kentwa.gov

Phone: 253-856-5834 or 206-573-1724

Date: 04/27/2023

Case: #23-5110

Information: Eluding and Street Racing Suspect

SOCIAL MEDIA 08/2022



Matthew N. SLOBODA

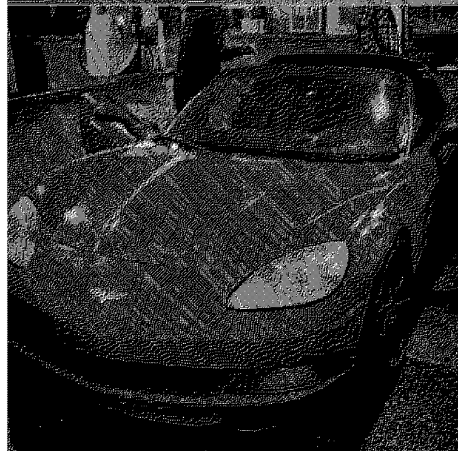
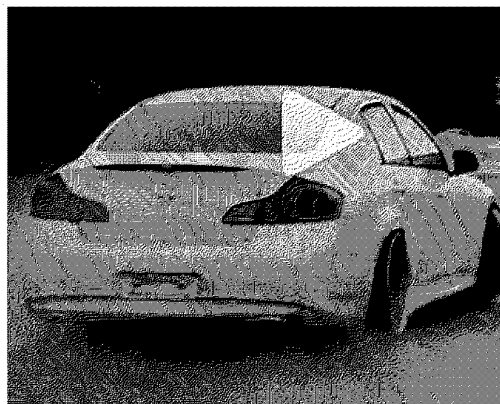
08/31/2001

3824 90th Ave. E., Edgewood

2012 Infiniti G37 (white)
WA: LEM403J

2006 Chevrolet Corvette
(red convertible)
CA: 6TEC929

**HISTORY OF
ELUDING
DWLS 3RD DEGREE
ACTIVE
MISDEMEANOR
WARRANT**



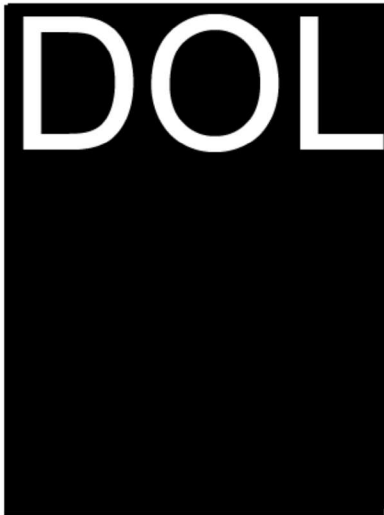
Matthew Sloboda is a frequent participant at illegal street race events in both Kent and Renton. Preliminary investigation has identified him as the driver of the pictured Infiniti G37 as well as the blue BMW M4 coupe seen in a viral video drifting around a marked police vehicle on 04/16/2023.

He also has history of attending street races in the pictured red Chevrolet Corvette (convertible).

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****

The blue BMW has been identified as belonging to Joshua Chuyeshkov

WA STATE DOL 09/22/2022



**Joshua M.
CHUYESHKOV**
10/22/2000

29541 200th Ct. SE,
Kent

2015 BMW M4 (blue)
WA: BRR7711



Please contact Commander Bava at 253-856-5834 or 206-573-1724 if Sloboda is contacted or the Infiniti or BMW are located. Kent Police will impound those vehicles for evidence.

There is no PC to arrest either subject at this time. The case remains under investigation.

Sloboda has an active misdemeanor warrant from Sumner Municipal Court (#2A0465206, DWLS 3rd degree, \$2,500 bail). Please confirm prior to arrest.

CYBER THREATS

(U) Cyber: New Credential-Stealing Malware Advertised on Telegram



(U) According to a US Naval Criminal Investigative Service (NCIS) Multiple Threat Alert Center (MTAC) Cyber Threat Division Threat Awareness Message (TAM) dated 21 APR 23, security researchers have identified two new variants of credential-stealing malware that are being advertised for sale via the Telegram platform. Credential-stealing malware can be extremely dangerous for victims, as it could allow malicious actors to bypass security measures for logging in, providing them with access to

numerous online accounts and an abundance of sensitive data. Malicious actors can use stolen credentials for a variety of follow-on operations ranging from financial theft to large-scale cyberespionage operations. Additionally, malicious actors commonly sell or post compromised credentials to underground forums, potentially making the credentials available to other threat actors worldwide.

(U) One of the newly identified variants of malware, dubbed "Zaraza Bot" by its developers, is being advertised on a popular Russian Telegram channel and likely rented on a subscription basis. Zaraza Bot can take screenshots from victims' devices and targets 38 different browsers including Google Chrome and Microsoft Edge, to steal login credentials for victims' email, banking, and other high-value accounts. Although the browsers typically encrypt stored passwords, according to reporting, Zaraza Bot is capable of decrypting them. Zaraza Bot then leverages Telegram as its command and control (C2) to transfer the stolen data back to the actors. Although the initial infection vector associated with Zaraza Bot

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****

is unknown, malicious cyber actors can use a variety of methods to distribute credential-stealing malware, including phishing emails, fake advertisements, and malicious apps.

(U) A second type of credential-stealing malware that has been recently advertised on Telegram has been dubbed "Legion" by its developers. The developers, who use the moniker "Forza Tools," have a large group of followers on their Telegram channel, as well as a YouTube channel which they use to post malware tutorials. Legion attempts to steal credentials for a variety of online accounts, primarily focusing on compromising email accounts, which can be used to send mass phishing emails. Legion is also capable of hijacking short message service text messages on compromised devices, likely to steal the content of text messages and to send malicious text messages to additional victims.

(U) Because Telegram allows users to remain anonymous and provides them with encrypted communications, cybercriminals and state-sponsored advanced persistent threat (APT) groups are increasingly using it to advertise malware for sale, distribute malware, and transfer stolen data. In the past year, security researchers have discovered multiple other types of malware and services that have been advertised via different Telegram channels, including Titan Stealer, MacStealer, and services that allow malicious actors to purchase malware bundles and "how-to" guides, such as the "Eternity Project" malware-as-a-service (MaaS).

(CUI) NCIS MTAC Cyber Threat Division Comment: NCIS assesses that while the newly observed credential-stealing malware currently poses a low threat to US Department of Navy networks and personnel, the threat may increase as the actors continue to promote the malware via Telegram channels and increase their customer base. NCIS assesses this with moderate confidence, based on reporting highlighting the increasing use of Telegram by malicious actors worldwide to buy and sell various types of malware. Many types of malware promoted on Telegram appear to be primarily focused on stealing credentials, as the credentials can be used in a wide range of malicious activities. Personnel should follow the below recommendations to help prevent an accidental malware download and protect accounts from a potential compromise.

- (U) Ensure devices are updated and running reputable antivirus software.
- (U) Refrain from opening emails, text messages, or social media messages from unknown or suspicious senders; regardless of whether the sender is legitimate, carefully review any content/links/attachments sent.
- (U) Go directly to reputable websites for information or account access rather than clicking on a link received by a third-party source.
- (U) Use multi-factor authentication when possible.
- (U) Refrain from saving credentials in browsers.
- (U) Use different password and username combinations for different accounts.
- (U) Use complex passwords and change them often.

Sources: (NCIS MTAC Cyber Threat Division, TAM, Product Number: NCIS-TAM-CYBR-N035-FY23, 21 APR 23) via ARMY THREAT INTEGRATION CENTER (ARTIC)

(U//FOUO) Cyber: Criminals Exploit Online Marketplaces to Engage in Carjackings and Resale of Stolen Vehicles



(U//FOUO) The FBI New Haven, in coordination with the FBI's Office of Private Sector (OPS), prepared this Liaison Information Report (LIR) to inform cross-sector partners about criminal actors engaged in carjackings using online marketplaces, mobile phone applications, and the enticement of cash purchases. The use of online marketplaces is appealing to criminal actors because online personas/profiles are easily created using minimal personally identifiable information, giving criminal actors anonymity from their victims. Additionally, by conducting cash transactions, criminal actors are incentivized by limiting the

*** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY ***

victim's recourse.

(U//FOUO) In one case, criminal actors created a social media profile using a moniker and negotiated the purchase price of a motor vehicle through an online marketplace. Upon completion of the test drive, the criminal actors brandished a firearm at the seller at the time of payment, demanded the title, and forced the seller out of the vehicle. Following the theft of the vehicle, the carjackers deleted the social media profile. The carjackers, now in possession of the stolen motor vehicle, created a second profile using a moniker on another online marketplace and advertised the vehicle for sale. The criminal actors negotiated the sale of the vehicle with a buyer, who also used a moniker on the online marketplace. Per the online marketplace records, after the sale was completed, the buyer re-contacted the criminal actors, questioned the legitimacy of the transaction, and demanded additional financial compensation, but the criminal actors did not respond. The buyer advised law enforcement they subsequently re-sold the vehicle and believed it had been shipped out of the country.

(U//FOUO) In another instance, the same criminal actors used the same modus operandi to carjack another victim and resell the stolen vehicle. Upon registering the vehicle, the unsuspecting buyer learned the vehicle had been reported stolen and attempted to contact the criminal actors. They discovered the criminal actors had changed their profile name to another moniker and the telephone number for re-contact was no longer in service.

(U//FOUO) While an indicator alone does not accurately determine a carjacking and resale scheme, the totality of behavior, message delivery, and other relevant circumstances should be evaluated when considering notification of security/law enforcement personnel.

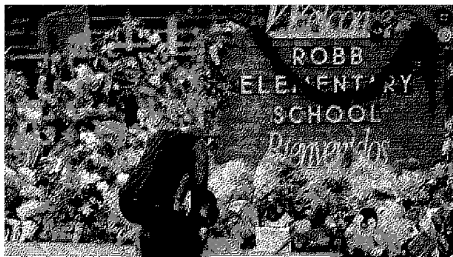
(U//FOUO) The following suspicious activities/indicators include but are not limited to any individual, group, or activity (observe these indicators in context and not individually):

- (U//FOUO) Increasing contact or presence of potential vehicle buyers or sellers on online marketplaces with newly created social media profiles with a limited history.
- (U//FOUO) Unsolicited contact from social media profiles with a nominal number of contacts and photos.
- (U//FOUO) Potential buyers or sellers of vehicles refusing to conduct a transaction at a police station or other established safe location; and
- (U//FOUO) Seller's advertising vehicles with "too good to be true" pricing or prices noticeably below the vehicle's estimated value.

(U//FOUO) The FBI's Office of the Private Sector disseminated this LIR; please direct any requests and questions to your FBI Private Sector Coordinator at your local FBI Field Office: <https://www.fbi.gov/contact-us/field-offices>. (FBI New Haven, in coordination with FBI's OPS, LIR, Product Number: LIR230413006, 13 APR 23) Source: via the Army Threat Integration Center (ARTIC)

PUBLIC SAFETY

FBI: Active Shooter Incidents Fell in 2022 but Remained Relatively High



The FBI is reporting a slight decline in the number of "active shooter" incidents last year but says the tally still surpassed the levels seen in most of the last five years. The FBI defines an active shooter as "one or more individuals actively engaged in killing or attempting to kill people in populated area" such as a school or nightclub.

The FBI is reporting a slight decline in the number of "active shooter" incidents last year but says the tally still surpassed the levels seen in

*** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY ***

most of the last five years.

The FBI defines an active shooter as “one or more individuals actively engaged in killing or attempting to kill people in a populated area” such as a school or nightclub.

Not all shootings are counted as active shooter incidents by the FBI. Excluded are cases of self-defense, gang violence, drug violence, and domestic disputes. In a report released on Wednesday, the FBI said it counted a total of 50 active shooter incidents in 2022, down from 61 the previous year.

But that number is still 67% higher than five years ago when there were 30 active shooter incidents in the country. “While we see a decrease from 2021 to 2022, we see over time, over the past 20 years since we’ve been reporting on active shooter incidents, and certainly in the last five years, there has been an overall increase in this number,” a senior FBI official said during a press call with reporters.

The biggest increase in recent years came in 2021. When the number of active shooter incidents jumped from 40 to 61, according to the report. Although fewer people died in active shooter incidents in 2022 than in 2021, the total casualty count — deaths and injuries combined — was higher last year than the year before. The shootings caused a combined 313 casualties, including 100 killed and 213 wounded, up from 243 in 2021, including 103 people killed and 140 wounded, the report said. Last year’s casualty count was the highest in five years, the report said. According to the report, 13 of the 50 incidents last year resulted in mass killings, defined as four or more people shot dead in single incident.

Not everyone agrees on what constitutes a mass shooting, however. The Gun Violence Archive uses a broader definition that encompasses incidents with at least four victims, either injured or killed. By this definition, the non-profit tallied 646 mass shootings last year, more than ten times the number reported by the FBI.

In its report, the FBI singled out four incidents that claimed the most lives or inflicted the most injuries last year.

On May 24, a gunman entered Rob Elementary School in Uvalde, Texas, opening fire on students and staff. Nineteen children and two adults were killed. It was the deadliest school shooting since 2012, when a gunman killed 20 children and six adults at Sandy Hook Elementary School in Newtown, Connecticut. Ten days before the Uvalde massacre, another gunman entered a supermarket in a predominantly African American neighborhood of Buffalo, New York, killing ten people and injuring three.

The two incidents with the highest number of injuries but fewer deaths occurred in Highland Park, Illinois, and Colorado Springs, Colorado.

On July 4, a gunman perched atop a commercial building fired into an Independence Day parade crowd, killing seven and wounding 48 others.

On November 19, five people were killed and 28 others wounded when a gunman opened fire in an LGBTQ club. The FBI says it tracks active shooter incidents to give law enforcement agencies and the public a baseline understanding of the problem.

This year’s report offers a wealth of details about the shooters, the time and location of the shootings, and the types of weapons used in the assaults.

Among the report’s key findings:

- Of the 50 shooters, 47 were male. They ranged in age between 15 and 70 years old. Four shooters wore body armor, while two acted as snipers.
- In nearly half of the incidents, the shooter had a known connection to the location, the victim or both.
- In the incidents, the shooters used a total of 61 weapons, including 29 handguns, 26 rifles, three shotguns, and three unknown firearms.
- The 50 active shooter incidents occurred in 25 states and the District of Columbia, with Texas reporting six incidents, more than any other state.

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****

The shootings took place in seven types of locations, including open spaces, commercial buildings, residences, educational facilities, government buildings, houses of worship, and a healthcare facility.

For 2021, FBI highlighted an emerging trend involving “roving active shooters,” or gunmen who shoot in multiple locations. That trend was observed in 2022 as well, the senior FBI official said without giving a number. Source: Homeland Security News Wire

Analyst Comment On 26 April, the Federal Bureau of Investigation (FBI) and the Advanced Law Enforcement Rapid Response Training Center (ALERRT) at Texas State University published a joint report titled “Active Shooter Incidents in the U.S. in 2022.” For the purpose of the report, the FBI defines an active shooter incident as one or more individuals actively killing or attempting to kill people in a populated area with a firearm. Shootings resulting from another criminal act, like gang violence or drug-related, are not counted as active shooter incidents. In 2022, the FBI designated 50 shootings as active shooter incidents, which is 18% lower than the number of incidents the U.S. saw in 2021 (61), but still 66.7% higher than the number of incidents reported in 2018 (30). Thirteen of the 50 incidents meet the federal criteria for a mass killing: three or more killings in a single incident. The 2022 active shooter incidents resulted in 313 casualties, substantially higher than the 243 casualties caused by active shooters in 2021. However, the number of deaths from active shooter incidents in 2022 (100) declined slightly from 2021 (103) despite the higher number of casualties. Two of the 50 incidents in 2022 occurred on transit infrastructure – the 17 March 2022 shooting on a Broward County bus in Florida, and the 12 April 2022 shooting at the 36th Street Station in Brooklyn, New York. The full report can be viewed at: <https://www.fbi.gov/file-repository/active-shooter-incidents-in-theus-2022-042623.pdf/view>

Source: Over the Road-Bus Intelligence Awareness Daily (OTRBIAD) Report.

NATIONAL

(U//FOUO) United States: Juveniles Will Likely Leverage Explosives Availability to Target Secondary Schools



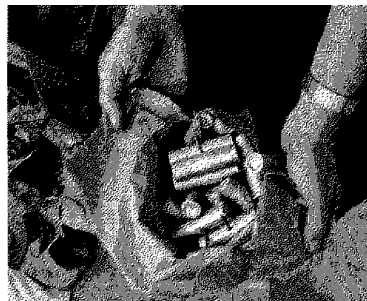
(U//FOUO) According to an FBI Bulletin dated 05 APR 23, the FBI assesses juvenile threat actors in the United States likely will leverage the availability of pre-made improvised explosive devices (IEDs), bomb-making materials, and IED construction instructions to target US secondary schools, resulting in student and staff casualties, and an erosion of public confidence in school officials and law enforcement (LE) personnel. This assessment is made with high confidence, based on open-source news reports; officers of other LE agencies; FBI agents with direct access; an FBI agent with direct access, who obtained the information from an interview of a subject; and an FBI agent with direct access, who obtained the information through legal process returns.

(U//FOUO) The FBI bases this assessment on the key assumptions explosive precursor chemicals (EPCs) will remain available through both physical retail stores and online vendors, and juveniles will maintain internet access to receive guidance for creating IEDs from online resources. The FBI further assumes most secondary schools in the United States have limited capability to detect the introduction of IEDs into the school's facility or setting. Finally, the FBI assumes IEDs are available to juveniles through in-person networks, legal fireworks stands, or complicit adults and legal guardians willing to acquire IEDs and bomb-making materials for juveniles who request them for purported entertainment purposes. If the FBI obtained information suggesting juveniles consider, but reject, the use of explosives in future school attacks, confidence in this assessment would decrease. If juveniles become aware of enhanced security measures nationwide to specifically screen for the attempted introduction of IEDs into school buildings, the likelihood of this assessment would decrease. In the long term, the FBI assesses juvenile threat actors likely will plan and successfully conduct complex attacks using IEDs in coordination with firearms when targeting US secondary schools to ensure their fame and notoriety, further complicating LE response to active shooter incidents.

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****

(U//FOUO) Juveniles Likely Will Leverage IED Availability to Target Secondary Schools, Resulting in Casualties and an Erosion of Public Confidence in School Officials and LE Personnel

(U//FOUO) The FBI assesses juvenile threat actors in the United States likely will leverage the availability of pre-made IEDs, bomb-making materials, and IED construction instructions to target US secondary schools, resulting in student and staff casualties, and an erosion of public confidence of school officials and LE personnel. This assessment is based on juveniles in Pennsylvania conspiring to attack their school using IED information obtained from the internet, a juvenile and their parent manufacturing an IED that inadvertently exploded in the juvenile's classroom, juveniles in Nebraska purchasing IEDs from a complicit adult, and juveniles across the United States plotting unconnected bombings against their schools, which LE disrupted.



- (U) Between May 2021 and October 2021, according to three open-source news reports, US LE officials arrested six juveniles for plotting to conduct attacks using IEDs against two high schools and another unidentified target. In two incidents, LE searches identified functional IEDs. In the third incident, an LE search found evidence of incendiary devices.

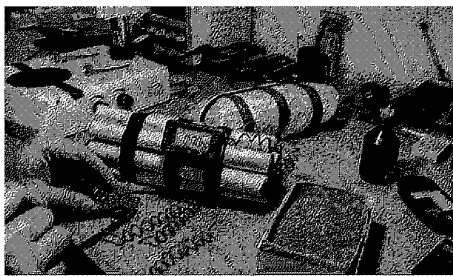
- (U//FOUO-LES) In September 2021, according to an open-source news report, LE officials in Pennsylvania arrested four juveniles for conspiring to attack their high school. The date of attack was planned for the 25th anniversary of the 1999 Columbine High School massacre in Colorado, which killed 13 students and teachers. They were charged with multiple violations, including unlawful possession of weapons of mass destruction (WMDs) and possession of explosive material. One of the juveniles possessed components for IEDs, IED-making instructions, and an incendiary device at their home. According to an officer of another LE agency, one of the juveniles used the internet to obtain instructions on how to construct IEDs.

- (U//FOUO-LES) According to an officer of another LE agency, on 08 MAR 21, a 16-year-old student accidentally detonated explosive materials he had brought to school for unknown purposes. According to an FBI agent with direct access, on 08 MAR 21, authorities conducted a search of the juvenile's home and found EPCs and bomb-making materials. A subsequent interview with the student and his father revealed they manufactured hex methylene triperoxide diamine (HMTD) from the chemicals found at the residence.

- (U//FOUO) According to an FBI agent with direct access, who obtained the information from an interview of a subject, in December 2021, multiple juveniles purchased illegal homemade fireworks from an adult residing in Omaha, Nebraska. According to an FBI agent with direct access, the adult's text message conversations from July 2021 identified the adult was aware his illegal homemade fireworks were sometimes purchased by juveniles who used them to destroy portable toilets on multiple occasions. Identified juveniles used the same homemade fireworks to destroy a stone mailbox with sufficient damage that local LE notified the Joint Terrorism Task Force, according to an FBI agent with direct access, who obtained the information through legal process returns.

(U) Perspective

(U//FOUO) LE continues to face multiple challenges with identifying juvenile IED threat activity in schools, including limited bystander reporting, juveniles' access to the internet, and school security practices. The FBI and National



Counterterrorism Center (NCTC) examined the role of bystanders in detecting terrorist activity. The FBI and NCTC identified family members and peers as the largest bystander groups but noted those groups most often communicate their concerns directly to the person of concern rather than LE. These individuals experience significant psychological barriers to making a report on their peer or family member to LE, leading to a majority of those bystanders not intervening to prevent acts of violence when they become aware of concerning behavior. For example, juveniles who purchased illegal homemade fireworks in Omaha attended multiple secondary schools in the Omaha

*** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY ***

metropolitan area. The students shared videos of off-campus property destruction caused from using the illegal homemade fireworks and advertised on social media, inviting other juveniles to witness future detonations of the devices in-person. Despite this awareness, neither the juvenile bystanders who attended the detonations in-person nor other juvenile bystanders who saw the advertisements but did not attend reported the incidents to LE or school officials. Although the illegal homemade fireworks used in Omaha did not represent a terrorist act and occurred off the school campus, the failure of multiple peer bystanders to report information about illegal use of explosive devices to LE or school officials highlights the remaining vulnerability for bystanders to report any violent activity.

(U) Juveniles have used their access to online websites and social media to freely communicate threats under the false pretext of anonymity. December 2021 featured a large number of violent threats, particularly related to shootings and bombings, made on social media against schools, which increased the LE presence at schools, public safety statements by school districts, and the disruption of school activities. Despite these increased precautions, school shootings in the United States increased to a record high of 55 in 2022, compared to the previous record of 35 in 2021.

(U//FOUO-LES) The assessment in this intelligence bulletin diverged from the analysis in the 28 DEC 22 FBI Strategic Perspective: Executive Analytic Report (SPEAR), titled “(U//FOUO) Juvenile School Bombing Plotters Detail Their Plans in Writing,” which assessed juvenile school bomb plotters provide insight into their plans through their private personal writings, allowing close contacts to identify and report violent plans. This bulletin differs from the SPEAR by indicating bystanders in some instances include complicit adults and legal guardians who provide juveniles access to bomb-making materials.

(U//FOUO) This intelligence bulletin aligns with the 13 SEP 21 Joint Counterterrorism Assessment Team First Responder’s Toolbox article, titled “(U) Intervention Options for Minors Vulnerable to Violent Extremism Activity.” In that product, NCTC, US Department of Homeland Security (DHS), and FBI assessed some minors were vulnerable to violent extremist messaging that appealed to a variety of developmental and psychological needs. NCTC further assessed either COVID-19 isolation or an increased use of social media by minors affects minors’ susceptibility to terrorist messaging. One example featured a minor who was arrested for preoperational online activities pertaining to information on bomb making and photos of IEDs. Although this intelligence bulletin does not focus on the extremist propaganda, it does align with the article’s assessment on juveniles’ online capabilities to obtain information and make connections with nefarious actors.

(U//FOUO) **FBI Comment:** In the long term, the FBI assesses juvenile threat actors likely will plan and conduct complex attacks using IEDs in coordination with firearms when targeting US secondary schools to ensure their fame and notoriety, further complicating LE response to active shooter incidents. The complexity, planning, and execution of school attacks continue to evolve toward greater violence and higher mortality rates as juvenile offenders switch from handguns to fully automatic weapons and IEDs and learn from past school shootings’ successes and failures. Federal, state, and local LE officials, mental health workers, and education personnel have the opportunity to work with school districts and state departments of education to develop procedures for schools to monitor student activity on their technology networks, provide training on research related to construction of IEDs, develop procedures for reporting suspicious activity, and create screening procedures for potential IEDs. Local threat assessment and threat management teams can further work with school districts through referrals to their internal threat assessment teams and maintain bi-directional communication with schools when concerns arise. Through engagement with suicide prevention hotlines and hotlines providing mental health support to teenagers, LE has the opportunity to develop additional procedures that preserve caller privacy while also identifying callers with the potential to use IEDs. Lastly, state fusion centers have the opportunity to expand the Nationwide Suspicious Activity Report Initiative to connect with anti-bullying hotlines present in some states to detect indicators of possible IED production.

(U//FOUO) **Indicators juveniles are planning complex attack with IEDs include:**

- (U//FOUO) Attending school with explosive residue on their personal items.
- (U//FOUO) Conducting explosive-related research on school computers without appropriate purpose or approvals.
- (U//FOUO) Discussing school attacks that are more deadly and cause more notoriety than previous attacks.

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****

- (U//FOUO) Posing unusual or suspicious questions during science courses related to EPCs, including handling procedures, procedures for acquiring such materials, and whether the school has such materials on hand.
- (U//FOUO) Theft of EPCs from school laboratories attributed to an enrolled student.
- (U//FOUO) Sharing videos of explosions and claiming credit for the explosions; and
- (U//FOUO-LES) Encouraging others to conduct explosive and firearm attacks against schools.

Sources; (FBI, Juveniles Likely Will Leverage Explosives: Availability to Target Secondary Schools, Bulletin, 05 APR 23) via the Army Threat Integration Center (ARTIC)



Pitt Researchers Collect Data on Where Train Accidents Occur and What They Threaten

[Pennsylvania] Railroad safety continues to be a concern after the East Palestine derailment in February and the train wreck in Harmar Township last May. A group of University of Pittsburgh researchers gathered data to identify where train derailments occur in southwestern Pennsylvania and the risk these accidents pose. The concern surrounding

train derailments is still top of mind. "After East Palestine, everyone was kind of like, 'what are we going to do next?'" said Daniel Bain, associate professor with the Geology and Environmental Science Department at the University of Pittsburgh. Bain felt compelled to start researching train accidents after the February derailment in East Palestine. Bain is one of the founding members of the Pittsburgh Water Collaboratory. Source; CBS, 4/26/2023

Analyst Comment Researchers at the University of Pittsburgh have been studying train derailment trends in Southwestern Pennsylvania by reviewing and plotting all rail accidents the Federal Railroad Administration (FRA) has for the region between 2011 and 2022. Their findings reportedly indicate that "211 of the 270 accidents were within 300 yards of a major river." According to a Pittsburgh Water Collaboratory report, 22% of train derailments in the region from 2011 to 2021 "involved HAZMAT cargo." When approached about the risks of water contamination, Allegheny County Emergency Services Chief Matt Brown said that the dangers posed are "not just with trains."

The most dangerous by volume and frequency is by vehicle. But all methods of transportation are included, such as river barge, pipeline, airplane, and trains." Brown also said that the assessed level of risk "can change based on method of transportation, product or chemical type, volume or amount of product, frequency of occurrence or potential and many times location or geography," and that from "the threat and risk perspective, flash flooding continues to remain [Allegheny County's] greatest potential risk."

Source; Over-the-Road-Bus Intelligence Awareness Daily (OTRBIAD) Report.

SSRIG Comment For us in the Pacific Northwest we have a lot of train traffic (mainly BNSF) that goes over multiple waterways and the largest is the Puget Sound. The same threats and risks mentioned above apply here for Emergency Management to consider in planning.

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****

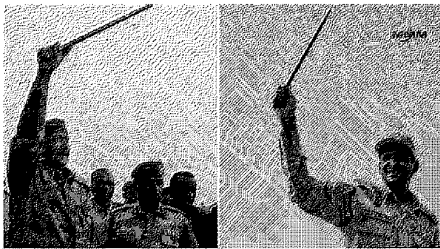
INTERNATIONAL

Germany Arrests 28-Year-Old Syrian Over 'Radical Islamist' Bomb Plot



[Hamburg, Germany] German authorities arrested a 28-year-old Syrian national on Tuesday morning, one of two brothers suspected of planning to blow up civilian targets using a homemade explosives belt for "radical Islamist and jihadist" reasons, a statement said. Public prosecutors in the northern port city of Hamburg carried out searches as part of a joint probe with police, arresting the man whom they believed bought raw materials for bomb-making off the internet over several weeks. Source; Reuters, 4/25/2023

Analyst Comment On 25 April, German police arrested a 28-year-old Syrian man in Hamburg, Germany on suspicion of planning to carry out an explosives attack motivated by Islamic extremism. According to the statement released by prosecutors, the 28-year-old man and his 24-year-old brother allegedly "planned an attack with a home-made explosive belt, out of a radical Islamist and jihadist motivation in order to carry out an attack against civilian targets." The man has not been named by authorities, and he was allegedly "helped and encouraged" by his 24-year-old brother who lives in Kempten, Bavaria. The 24-year-old brother was also detained by German authorities during the investigation. Investigators believe the men had been purchasing raw bomb-making materials off the internet for several weeks. Authorities have not remarked on any specific targets the man may have had, but during the investigation over 250 police searched properties in Hamburg and Kempten where they seized "large amounts of evidence including chemical substances." Source; Surface Transportation & Public Transportation ISAC Transit & Rail Intelligence Awareness Daily Report (TRIAD)



Sudan in Chaos

For the last two weeks, two generals and their armies have been locked in a power struggle in Sudan, mostly in the capitol of Khartoum. Intense fighting has forced foreign governments and the UN to evacuate their citizens from embassies and international organizations, reports BBC. The conflict has shutdown normal life and created a humanitarian crisis. Seventy percent of the hospitals are not functioning, a laboratory containing infectious diseases was seized creating a possible biological hazard, and food and fuel are becoming scarce. The struggle pits one general, Abdel Fattah al-Burhan, who controls the Sudanese Army against Mohamed Hamdan Dalgo, who commands the Rapid Support Forces (RSF). The RSF is connected to war crimes and has links to the Russian Wagner Group. The disintegration into a civil war could have significant impacts on neighboring fragile nations and present opportunities for extremist groups to exploit.

Analyst Assessment The UN World Food Programme (WFP) warned that the violence in Sudan, where a third of the country already struggles with food shortages, has the potential to push millions into a famine. A recent report focused on the link between food insecurity and conflict, found that extremist groups use opportunities providing food and resources to drive recruitment. The WFP also warned that up to 13 million Afghans are experiencing famine attributed to state violence, political mismanagement, and waning international support. Information found in the Discord leak revealed that ISIS-K operating in Afghanistan was consolidating and plotting attacks on western targets like embassies, churches and business centers. On Tuesday, German security forces in Hamburg arrested two Syrian brothers planning an explosive attack motivated by Islamic extremism. Currently this past week or more two Americans have been killed during this crisis. Source; Watchline@fdny.nyc.gov

*** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY ***

Other National/International Articles of Interest (Links):

United States: Two Men Sentenced For Planning To Attack U.S. Electric Substations

<https://www.dispatch.com/story/news/courts/2023/04/21/white-supremacists-sentenced-in-ohio-for-plot-to-attack-power-grid/70140160007/>

The ABCs of AI: 20 key terms every police officer should know

<https://www.police1.com/artificial-intelligence/articles/the-abcs-of-ai-20-key-terms-every-police-officer-should-know-BJIDkqEk32RrPvYf/>

160,000 rounds of ammo stolen from Ohio Police Division

<https://www.wtrf.com/top-stories/160000-rounds-of-ammo-stolen-from-ohio-police-division/>

Worldwide: Critical Infrastructure Hit By Supply Chain Attack Behind 3CX Breach

<https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise>

'Coma in a Bottle': Custom, border patrol officers seize 6 gallons of liquid ecstasy in Philadelphia

<https://6abc.com/coma-in-a-bottle-liquid-ecstasy-philadelphia-gamma-butyrolactone-chemical-seized-date-rape-drug/13189641/>

3 high schoolers charged with 1st-degree murder in rock-throwing incidents

<https://6abc.com/3-high-schoolers-charged-with-1st-degree-murder-in-rock-throwing-in/13189683/>

Guardzman in leak case wanted to kill a 'ton of people': US

<https://apnews.com/article/leaked-documents-air-national-guardzman-jack-teixeira-d7c8dbaeb3b7a5ae69faeab04ede2ab0>

What cops can learn from YouTube

https://www.police1.com/police-training/articles/what-cops-can-learn-from-youtube-XvqTTYE5WGXXsTRL/?utm_source=Police1&utm_campaign=b4e105a82f-EMAIL_CAMPAIGN_2023_04_27_07_12&utm_medium=email&utm_term=0_5584e6920b-6f9733b5d3-%5BLIST_EMAIL_ID%5D

*TPD/PCSD Homeland Security Reports Received this week 7.

*** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY ***

To: SHRCOMMISSIONED[SHRCOMMISSIONED@piercecounitywa.gov]; SHRJCO[SHRJCO@piercecounitywa.gov]
Cc: David Hutchinson[david.hutchinson@piercecounitywa.gov]
From: Gary Smith
Sent: Fri 5/5/2023 3:52:52 PM
Subject: SSRIG Weekly Intelligence Summary 18 - 2023 (May 05, 2023)
Received: Fri 5/5/2023 3:53:01 PM
[SSRIG Weekly Summary 18-2023.pdf](#)

South Sound Regional Intelligence Group SSRIG email: PCINTEL@piercecounitywa.gov Weekly Summary		
#18-2023		May 05, 2023
Gary Smith Intelligence Analyst Gary.Smith@ci.tacoma.wa.us (253) 594-7964		This document is a FOUO communication and is not to be disseminated outside of the law enforcement or intelligence communities. Dissemination to media sources is not authorized.

REGIONAL

ERO Seattle Removes Convicted Terrorist

(U//FOUO) The Oregon TITAN Fusion Center and FBI Portland are Providing Information About “Suicide Kits” Mailed to Oregon Residents

OFFICER SAFETY

OMG - GANG EVENT – OFFICER SAFETY

Probable cause to arrest DV assault suspect

OFFICER SAFETY CONCERN – ARMED SUBJECT WITH MULTIPLE LE CONTACTS

OFFICER AWARENESS

PC to Arrest- Puyallup PD

Arrest Warrant for Robert Allen Post

CYBER THREATS

ABCs of AI: 20 Key Terms Every Police Officer Should Know

Millions of patients’ data confirmed stolen after Fortra mass-hack

PUBLIC SAFETY

Largest International Operation Against Darknet Trafficking of Fentanyl and Opioids Results in Record Arrests and Seizures

NATIONAL

CA: Metro Responds to Rising Crime with More Drug Arrests and 'Transit Ambassadors

Railroads Warned About Dangers of Longer Trains

INTERNATIONAL

DEA Operation Last Mile Tracks Down Sinaloa and Jalisco Cartel Associates Operating within the United States

Kremlin Drone Attack

Other National/International Articles of Interest (Links):

Gary L. Smith

Gary L. Smith
Criminal Intelligence Analyst
Regional Intelligence Group
TPD/PCSD
Tacoma, WA
(253) 594-7964
(253) 405-6214 (C)
gary.smith@cityoftacoma.org
gary.smith@piercecounitywa.gov

"There must be a Lone Ranger!"



*** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY ***



**TACOMA /PIERCE COUNTY
REGIONAL INTELLIGENCE
UNIT**



18-2023

Friday, May 05, 2023

WEEKLY SUMMARY

Det. Sgt. John Delgado (253) 341-1369
john.delgado@pierccountywa.gov

Gary L. Smith, Intel Analyst
gary.smith@cityoftacoma.org (253) 594-7964

***** SENSITIVITY NOTICE *****

This document is intended exclusively for the individual or entity to which it is addressed. This communication may contain information that is law enforcement sensitive, proprietary, privileged, confidential and may be legally protected or otherwise exempt from disclosure. If you are not the intended recipient, you are hereby notified that any disclosure, dissemination, copying or distribution of this transmission is strictly prohibited. If you have received this message in error, please notify the sender immediately by email and delete all copies of this message.

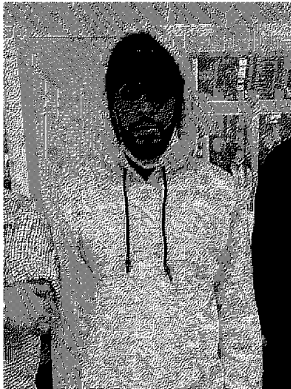
**The SSRIG is a member of the Joint Terrorism Task Force. Agencies in Pierce County are encouraged to forward information first to The SSRIG and we'll be sure to forward the information accordingly.

Please treat this and all other communications from this Regional Intelligence Unit as **LAW ENFORCEMENT SENSITIVE**. Further distribution of this document is restricted to law enforcement agencies, intelligence agencies, and Department of Defense organizations only, unless prior approval of this office has been obtained.

THIS DOCUMENT OR ANY SEGMENT THEREOF, MAY NOT BE RELEASED TO ANY MEDIA SOURCES.

REGIONAL

ERO Seattle Removes Convicted Terrorist



SEATTLE — Officers with U.S. Immigration and Customs Enforcement's (ICE) Enforcement and Removal Operations (ERO) Seattle removed Omer Abdi Mohamed, 38, a citizen of Somalia convicted of conspiracy to provide material support to terrorists, to his home country April 28.

A grand jury indicted Mohamed for conspiracy to provide material support to terrorists; providing material support to terrorists; and conspiracy to kill, kidnap, maim and injure Nov. 19, 2009. He was convicted of that charge and sentenced to 12 years in prison and 20 years of supervision by the U.S. District Court-District of Minnesota May 29, 2013.

"The immigration court's judgement for Mohamed's removal shows those who seek to support terrorism in any form will not find safe haven or privilege in the U.S.," said ERO Seattle Field Office Director Drew H. Bostock. "ERO officers continue to keep our communities safe by using the best information available to find, and remove, public safety threats from our community."

ERO officers encountered Mohamed while he was in the Federal Bureau of Prisons' custody at the Greenville Federal Correctional Institution in Illinois Aug. 1, 2018, and placed an immigration detainer the same day. Mohamed was released from the Bureau of Prisons' custody at the Federal Detention Center in SeaTac, Washington, and taken into ERO custody Feb. 21. He was ordered removed to Somalia by an immigration judge with the Department of Justice's Executive Office of Immigration Review March 8. Mohamed was repatriated to Somalia April 28 without incident.

*** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY ***

In fiscal year 2022, ERO arrested 46,396 noncitizens with criminal histories. This group had 198,498 associated charges and convictions, including 21,531 assault offenses; 8,164 sex and sexual assault offenses; 5,554 weapons offenses; 1,501 homicide-related offenses; and 1,114 kidnapping offenses.

As one of ICE's three operational directorates, ERO is the principal federal law enforcement authority in charge of domestic immigration enforcement. ERO's mission is to protect the homeland through the arrest and removal of those who undermine the safety of U.S. communities and the integrity of U.S. immigration laws, and its primary areas of focus are interior enforcement operations, management of the agency's detained and non-detained populations, and repatriation of noncitizens who have received final orders of removal.

ERO's workforce consists of more than 7,700 law enforcement and non-law enforcement support personnel across 25 domestic field offices and 208 locations nationwide, 30 overseas postings, and multiple temporary duty travel assignments along the border.

Members of the public can report crimes and suspicious activity by dialing 866-347-2423 or completing the online tip form. Learn more about ICE's mission to increase public safety in your community on Twitter @EROSSeattle. The Seattle area of responsibility covers Washington, Oregon and Alaska. Source: <https://www.ice.gov/news/releases/ero-seattle-removes-somali-citizen-convicted-supporting-terrorism>

OREGON TITAN FUSION CENTER
FEDERAL BUREAU OF INVESTIGATION - PORTLAND
JOINT SITUATIONAL AWARENESS BULLETIN



Situational Awareness Bulletin

3 May 2023



(U) THIS PRODUCT EXPRESSES THE PERSPECTIVE OF FBI PORTLAND FIELD OFFICE AND MAY NOT BE REFLECTIVE OF THE NATIONAL PERSPECTIVE OF THE FBI.

(U) THE INFORMATION IN THIS DOCUMENT MAY NOT BE UPLOADED TO ANY DATABASES, USED FOR ANY PURPOSES, OR DISSEMINATED TO ANY OTHER RECIPIENT WITHOUT THE ADVANCED JOINT AUTHORIZATION OF THE OREGON TITAN FUSION CENTER AND FBI.

This bulletin may contain information designated as "for official use only" (FOUO), "law enforcement sensitive" (LES), and/or controlled information. Pursuant to OAR 137-090-0130, Do not forward or disseminate to any individual or group that does not have a valid right to know/need to know. Any request for copies of this bulletin should be directed to the FBI Portland field office or the OTFC.

(U//FOUO) The Oregon TITAN Fusion Center and FBI Portland are Providing Information About "Suicide Kits" Mailed to Oregon Residents

(U) Executive Summary

(U//LES) The Oregon TITAN Fusion Center (OTFC) and FBI Portland are releasing this bulletin to advance law enforcement agencies' awareness of Oregon residents receiving "suicide kits" including sodium nitrate pills and instructions on how to commit suicide from an identified Canada-based individual. Law enforcement agencies receiving requests for welfare checks or other suicide-related investigative activities are asked to report findings to the FBI and Fusion Center and to maintain records related to any response or investigative activity.

(U) Suicide Kit Composition and Distribution

(U//LES) Canadian authorities identified a subject who mailed hundreds of suicide kits to individuals worldwide; these kits were linked to dozens of subsequent suicides. Victims contacted the subject online and received the kits via mail.

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****

Suicide kits included sodium nitrate pills as well as instructions on how to commit suicide. Sodium nitrate is legal, readily available to the public, and commonly used in meat curing.

(U//LES) The FBI received information from Canadian authorities identifying potential victims in the United States. FBI Portland is identifying those based in Oregon to coordinate welfare checks with appropriate law enforcement agencies.

(U) Requested Actions

(U) Agencies receiving requests for welfare checks are requested to ask victims the following questions once standard welfare check protocols are completed.

- (U) How did the victim learn of the suicide kit?
- (U) Did the victim communicate directly with anyone about how to use the kits or were instructions provided in the kit itself?
- (U) If the victim communicated with someone about the kit usage, what communication channels were used (i.e., email, phone, messaging application, online, etc.)?
- (U) How were payments for the kit made to the seller?

(U) Agencies conducting welfare checks are asked to collect suicide kits from Oregon victims and coordinate disposition by contacting the FBI and OTFC using the contact information below.

(U) Agencies conducting welfare checks are asked to maintain records of response activity, collect communications between victims and the seller of suicide kits, and maintain records related to any investigation occurring in response to these welfare checks for potential future prosecutions.


(U) If your agency is not notified of a suicide kit recipient in your area but encounters a kit during regular activities, please contact the FBI and OTFC using the contact information listed below.

(U) FBI Portland can be reached directly at (503) 224-4181.

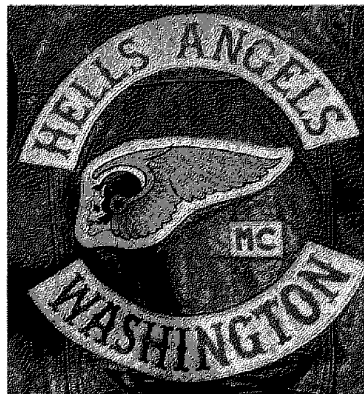
(U) OTFC: ofc@doj.state.or.us.

Source: Titan Fusion Center & FBI

OFFICER SAFETY

	Seattle Police Department	CONFIDENTIAL POLICE USE ONLY
---	---------------------------	---

OMG - GANG EVENT – OFFICER SAFETY



*** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY ***

EVENT: On May 6, 2023, at 1300 hours, the Hells Angels Motorcycle Club Seattle Chapter will be holding their yearly May Day party at Slim's Last Chance Saloon at 5606 1st Ave S, Seattle. Depending on the weather, this event has been known to attract crowds of 75-200, Hells Angels supporters and friendly motorcycle gangs such as the Bandidos, Gypsy Joker, Road Brother, Resurrection, Free Souls, Outsiders, and others.

OFFICER SAFETY: The Hells Angels Motorcycle Club is friendly with the Bandidos Motorcycle Club and both the Hells Angels and Bandidos are at war with the Mongols Motorcycle Club and Pagans Motorcycle Club, who are both friendly with each other and have formed an alliance. The Hells Angels have been fighting with the Mongols since 1977 and the Pagans since 1968. Tension and fighting between the Bandidos and Mongols and Pagans has been going on for approximately 3 years 2020.

CURRENT PICTURE:

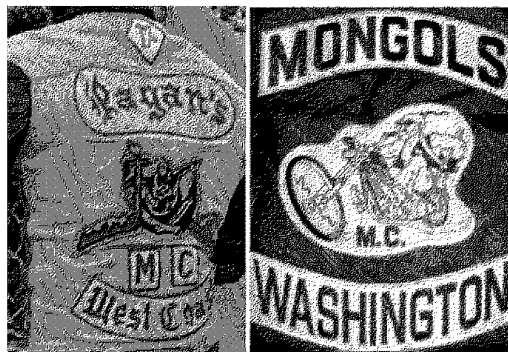
April 30, 2022, two large groups of Pagans and Hells Angels have a standoff in front of the Hells Angels Washington Nomads clubhouse in Spokane, WA and Spokane PD intervenes before violence starts and deescalates the heated incident.

May 14, 2022, 30 -40 Hells Angels and support club members ride in and attack a group of Pagans have a motorcycle event at their clubhouse in Fall River, Massachusetts. Seven (7) Pagans are stabbed and beaten and sent to the hospital in critical condition.

July 14, 2022 – Two Pagans from the Tri Cities, WA Chapter forced a road rage incident with three members of a Bandido Support Club called Anonymous MC which became a gun battle. One Pagan was killed, and one Anonymous MC Prospect was shot.

August 28, 2022 – A group of ten to twenty Hells Angels attempted to box in two Pagans Seattle Chapter members at a gas station in Kennewick, WA. The Pagans fled and one was chased down by Hells Angels members and physically assaulted on the highway. Another Hells Angel produced a firearm and attempted to shoot the Pagans as they rode away.



In the last year, both the Mongols and Pagans have expanded in Washington State and in the Seattle area and the Mongols Motorcycle Club has a gang event planned for May 13th, 2023, in the Seattle/Tacoma area at a unknown location. Additionally, as of the last week in March 2023, members of the Mongols were observed riding through Seattle on I-5 during rush hour which has not happened since the Mongols Seattle Chapter was formed in 2019. Throughout 2022 and into 2023, the President of the Pagans Motorcycle Club Seattle Chapter has routinely ridden through the SODO District in areas known to attract Hells Angels and Bandidos as if he is trying to be confronted.



EXPECT: As they have done at past events at Slim's Last Chance, the Hells Angels will likely post armed guards on the four corners surrounding the event. They will likely be Prospective members or associates and they may be armed with a variety of legal and/or illegal weapons, such as firearms, daggers, knives, axe handles, hammers, mag-lights, whips, and brass knuckles. The Hells Angels have in the past used armed security in vehicles with no gang markings to conduct patrols and surveillance around their events. You may also encounter subjects wearing body armor.

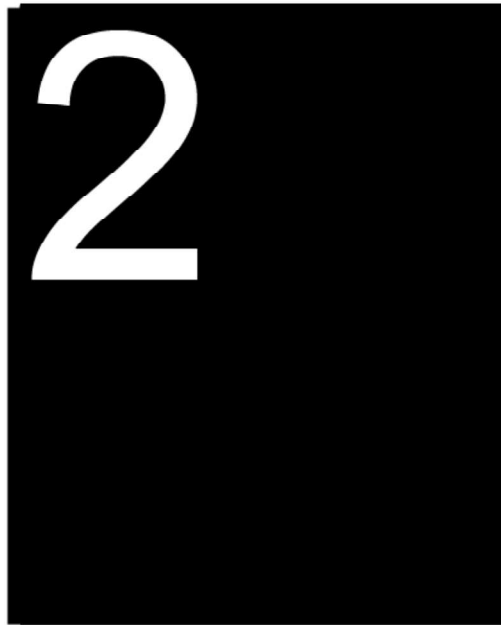
POTENTIAL ISSUES: The Mongols and Pagans are beginning to be more visible in the Seattle area and these gangs will often monitor each other's social media postings and know when and where the other is holding an event. It is possible that either the Mongols, Pagans or both could try to disrupt the Hells Angels event or to attempt to instigate a confrontation. The Mongols have also been known to send one or two members of their gang to the bars of their rivals in order to draw the rival gang to the location to confront their members at which time the Mongols have ambushed their enemies from cargo vans and other vehicles.

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****

	<h1>Special Bulletin</h1> <h2>TACOMA POLICE DEPARTMENT</h2> <p>Bulletin Number: S23-065</p> <p>May 5, 2023</p>	
<p>Detective Patrick Brame #272 Tacoma Police Department Special Victims Unit</p>	<p>Office – 253-591-5941 Cell – 253-405-5527 Email – Pbrame@cityoftacoma.org</p>	

Probable cause to arrest DV assault suspect

TPD case # 23-096-02467, 23-058-02373, 23-120-00106, 23-068-01227, 23-079-02223, 23-076-02674, 23-099-01438 and 23-074-02052



Probable cause to arrest **JAMES ARTHUR EVERETT** (DOB 04/01/1974) for 1 count Assault 1st degree (DV), 4 counts Assault 2nd degree (DV), 2 counts Burglary 1st degree (DV), 2 counts Felony Harassment (DV), 2 counts Harassment (DV) and 1 count of Stalking (DV). Everett has been charged with the above listed charges. Everett is homeless but is known to stay in the area of South 17th and G Street. Victim stated that during the latest assault, EVERETT was armed with a handgun. If located, please book on listed charges. A charging sheet will be at the desk at TPD OPS along with a probable cause statement.

Everett should be considered armed and dangerous.

Please email Det. Brame at Pbrame@cityoftacoma.org if Everett is arrested. (Desk) 253-591-5941, (Cell) 253-405-5527

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****



**Pierce County
Sheriff's Department
CRIMINAL INVESTIGATIONS DIVISION**

**SPECIAL
BULLETIN**

PCSD CIB 23-028s

PCSD CRIMINAL INVESTIGATIONS DIVISION

May 3, 2023

**OFFICER SAFETY CONCERN – ARMED SUBJECT WITH MULTIPLE LE
CONTACTS**

The Pierce County Sheriff's Department is advising law enforcement to use caution with regard to, Mauro Lopez Lopez (09-18-81), who recently has been contacted by law enforcement multiple times and was arrested last night for Eluding (PCSD Case #: 23-123-00031).

On 04/5/23 Mauro Lopez-Lopez, fired his gun in the air in front of his brother's house located at 244 161st St S. Deputies could not locate the firearm and he was released as a Suspect Verified for Weapon - Discharge From Vehicle or Street. (Case# 2309502470)

On 04/25/23 Mauro was also contacted by day shift where he had a "black semi-automatic handgun" on his front passenger seat" but was not actively committing a crime and refused to speak with deputies. (Case# 2311500862)

On 04/26/23 Mauro was reported for harassing employees at Good Vibes Espresso 15008 Pacific Ave S. (Case# 2311600285)

VEHICLE: Mauro is driving a dark blue Hyundai Sonata (WA-BYG0812).

There is NO PROBABLE CAUSE for Mauro; this information is for Officer Safety only.

2

NAME: Lopez Lopez, Mauro

DOB: 09-18-1991

PHY: 5'9" 220lbs Blk/Bro

SMT: TAT Chest - Lt: (Gabiella); TAT Side - Rt: (heart w/ cross)

LKA: Homeless but stays with brother at 244 161st St S, Spanaway, WA 98387



VEH: Dark Blue Hyundai Sonata WA- BYG0812

CHRI: Res Burg in 2014

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****

OFFICER AWARENESS

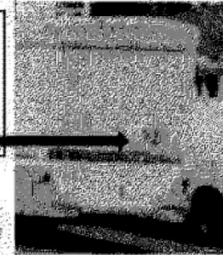
*** CONFIDENTIAL *** LAW ENFORCEMENT USE ONLY *** DISPOSE OF PROPERLY ***

	<h1>Special Bulletin</h1> <h2>PUYALLUP POLICE DEPARTMENT</h2> <p>Case Number: 2310500974</p> <p>Wednesday, May 3, 2023</p>	
Bulletin approved by Capt. J. Visnow		Prepared by Heidi Crawford (253) 770-3357 heidi.c@puyallupwa.gov

2



Decal on rear of motorhome is in the shape of the United States with some individual state shapes around it – such as a bumper sticker that would indicate all the states the vehicle has traveled.



Det. Stevens has developed probable cause to arrest James R. Door, 2/4/1965 for a Residential Burglary that occurred in Puyallup on April 15, 2023. In the process of breaking in he caused extensive damage to the victim's home by using a chainsaw to cut a hole in the floor from the crawl space. He broke a water line in the process and flooded the entire crawl space. He stole a significant amount of money and jewelry.

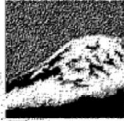

This motorhome is also the suspect vehicle in an unsolved burglary series in the Ocean Shores area, and it is believed James Door is the one committing the burglaries in both Puyallup and in Ocean Shores. Probable cause exists for James Door for the crimes of Residential Burglary, Trafficking in Stolen Property 1st, Malicious Mischief 1st, and Theft 1st. There is also probable cause to confiscate the vehicle for a search warrant.

If you locate Mr. Door or his vehicle, please contact Detective Travis Stevens at 253-466-8595 or Sgt. Kevin Gill at 253-954-6936. If you have nonurgent information regarding this subject or vehicle, you can email Det. Stevens at tstevens@puyallupwa.gov or Sgt. Gill at k.gill@puyallupwa.gov.

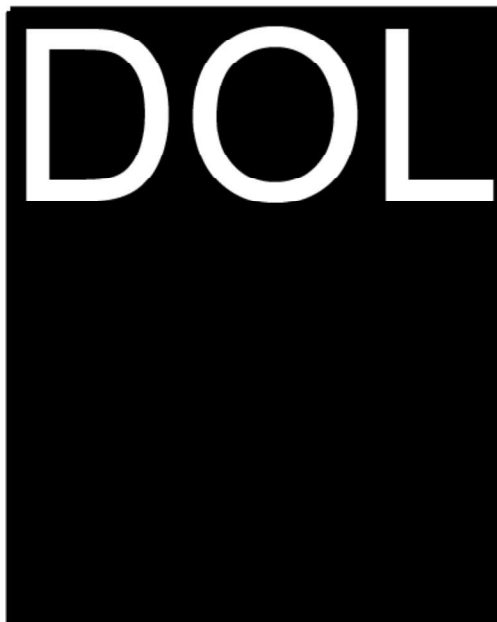
Puyallup Police Department 311 West Finness Puyallup, WA 98371 253-841-6415

*** CONFIDENTIAL *** LAW ENFORCEMENT USE ONLY *** DISPOSE OF PROPERLY ***

*** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY ***

 <p>Tacoma</p>	<h1>Special Bulletin</h1> <h2>TACOMA POLICE DEPARTMENT</h2> <p>Bulletin Number: S23-063 Wednesday May 3rd, 2023</p>	
<p>Det. Y. Song 093 Tacoma Police Department Traffic Unit</p>	<p>Office (253) 591-5910 Cell (253) 732-4807 Email ysong@cityoftacoma.org</p>	

Arrest Warrant for Robert Allen Post
TPD #23-102-00736



Robert Allen Post
DOB; 04/16/1993
 5'07", 161 lbs, blue eyes
LKA; 2034 E 34th St, TAC

On 4/12/23, a stolen BMW sedan crossed over the center lane and struck a victim vehicle head-on near 1625 S Tacoma Way. The driver of the BMW fled on foot after the collision and the passenger in the victim vehicle remains in critical condition.

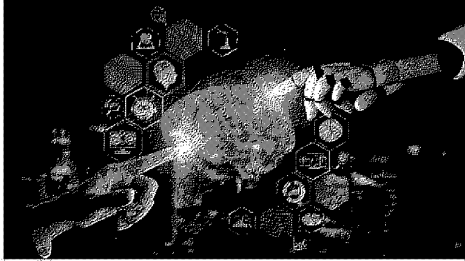
The driver of the BMW was identified as Robert A Post (DOB 4/16/93) and Felony Warrants has been issued by the Pierce County Prosecutor's Office for; Theft of a Motor Vehicle, Fail to Remain at Injury Accident, Identity Theft First Degree, and Duty in Case of Personal Injury or Death or Damage to Attended Vehicle or Other Property.

If Robert Post is located, confirm the warrants and arrest. Please notify Det. Y. Song at (253-732-4807) or ysong@cityoftacoma.org.

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****

CYBER THREATS

ABCs of AI: 20 Key Terms Every Police Officer Should Know



The use of artificial intelligence (AI) tools is rapidly transforming the field of law enforcement, allowing police officers to work more efficiently and effectively. A glossary of AI terms was generated by ChatGPT, a large language model that uses advanced machine learning algorithms to understand and respond to natural language inputs, making it a powerful tool for a range of applications, including law enforcement. With ChatGPT, police officers can quickly and easily access information about AI technologies and their applications in law enforcement, helping them to stay up to date on the latest developments in the field.

Some key terms are listed as:

- **Artificial Intelligence (AI):** The development of computer systems that can perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and language translation.
- **Predictive Policing:** The use of data analysis and AI tools to identify and prevent crime before it occurs, by analyzing patterns and trends in crime data to predict where and when crimes are most likely to occur.
- **Crime Pattern Analysis:** The use of data analysis and visualization tools to identify patterns and trends in crime data, enabling law enforcement to make more informed decisions and allocate resources more effectively.
- **Cybersecurity:** The protection of computer systems and networks from theft, damage, or unauthorized access, using a range of techniques and tools, such as encryption and firewalls.

For the rest of the 20 click on the link below: Source: Police1

<https://www.police1.com/artificial-intelligence/articles/the-abc-of-ai-20-key-terms-every-police-officer-should-know-BJIDkqEk32RrPvyf/>



Millions of patients' data confirmed stolen after Fortra mass-hack

Over five million people across the United States had personal and health information stolen in a mass-hack targeting dozens of companies, including healthcare providers, according to new filings with the federal government, media reported Thursday TechCrunch.

NationBenefits, a Florida-based technology company that offers supplementary benefits to its 20 million-plus members across the U.S., confirmed in April that hackers had stolen member data as the result of a mass ransomware attack targeting customers who used Fortra's GoAnywhere file-transfer software.

A listing on the U.S. Department of Health's data breach portal confirms that more than three million NationBenefits members had data stolen in the incident, including customer databases that include members' names, addresses, phone numbers, dates of birth, gender, marital status, and insurance details U.S. Department for Health and Human Services

The hackers also hit Brightline, a virtual coaching and therapy provider for children. The Department of Health's breach portal suggests more than 960,000 of the company's pediatric mental health patients had protected health and personal data stolen in the cyberattack.

U.S. healthcare giant Community Health Systems in February was the first to confirm that hackers had stolen data from its Fortra system, noting that hackers had accessed the personal data of at least one million patients. Source; TechCrunch

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****

PUBLIC SAFETY

Largest International Operation Against Darknet Trafficking of Fentanyl and Opioids Results in Record Arrests and Seizures



May 2, 2023 (DOJ). Washington, DC - Today, the Department of Justice, and its Joint Criminal Opioid and Darknet Enforcement (JCODE) team and international partners, announced the results of Operation SpecTor, which include 288 arrests, the most ever for any JCODE operation and nearly double that of the prior operation. Law enforcement also conducted more seizures than any prior operation, including 117 firearms, 850 kilograms of drugs that include 64 kilograms of fentanyl or fentanyl-laced narcotics, and \$53.4 million in cash and virtual currencies. Operation SpecTor was a coordinated international effort spanning three continents to disrupt fentanyl and opioid trafficking on the darknet, or dark web. The operation was conducted across the United States, Europe, and South America, and was a result of the continued partnership between JCODE and foreign law enforcement against the illegal sale of drugs and other illicit goods and services on the darknet. Operation SpecTor builds on the successes of prior years' operations and takedowns of marketplaces, which result in the seizure of darknet infrastructure providing investigators across the world with investigative leads and evidence. JCODE and Europol's European Cybercrime Centre (EC3) continue to compile intelligence packages to identify entities of interest. These leads allow U.S. and international law enforcement agencies to identify darknet drug vendors and buyers, resulting in a series of coordinated, but separate, law enforcement investigations, resulting in the statistics announced today. Source; <https://www.justice.gov/opa/pr/largest-international-operation-against-darknet-trafficking-fentanyl-and-opioids-results>

NATIONAL

CA: Metro Responds to Rising Crime with More Drug Arrests and 'Transit Ambassadors'



[Los Angeles, California] A month ago, LA Metro extended contracts with three policing agencies and expanded the roster of its security officers in an effort to reduce rising crime on buses, trains and transit stations so that riders who had left the system, because they don't feel safe, would return. But reports released on Thursday, April 27 by Metro indicate that police and sheriff deputies and Metro's Transit Security Officers were busy dealing with assaults and drug abuse as crimes spiked in the first quarter of this year. The number of crimes reported from March 21, 2022 to Feb. 22,

2023 totaled 3,267, about a 15% increase from the same period the year before. In February of 2023, crimes on the county transit system rose 21% compared to February 2022, Metro reported. During a roughly six-month period from September 2022 through February 2023, crime rose by 8%. The biggest increase in crime was drug use. Source; Mass Transit Magazine, 5/2/2023

Analyst Comment On 23 March, the Los Angeles Metro (LA Metro) board extended law enforcement contracts for up to three additional years and approved a plan to hire 48 additional Metro Transit Security Officers tasked with patrolling high-crime bus routes and train stations. Serious crime on LA Metro trains, buses, and transit properties increased by 24% in 2022, and January 2023 saw a 25% increase in crime from January 2022. In 2022, LA Metro also saw a "99% increase in year over-year complaints of passengers possessing or using illegal drugs." According to Metro's Chief Safety Officer, Gina Osborn, the expanded efforts by law enforcement on the LA Metro infrastructure over the past eight weeks have resulted in a "7% drop in reports to its call centers, and a 15% drop in customer complaints via the agency's Transit Watch app." During this same time frame, law enforcement made over 280 drug-related arrests on the LA Metro in addition to issuing 224 citations and 110 warnings. According to the LA Metro, since the hiring of additional transit security personnel and transit ambassadors, there has been a decrease in property theft, arson, and vandalism on LA Metro

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****

property, as well as a decrease in assaults against bus and train operators. Source; Over the-Road-Bus Intelligence Awareness Daily (OTRBIAD) Report.



Railroads Warned About Dangers of Longer Trains

Federal regulators are warning railroads that the long trains they favor can cause all kinds of problems and contribute to derailments, so they want the railroads to ensure their training and operating procedures account for that. The Federal Railroad Administration stopped short of recommending in its latest safety advisory issued Thursday that railroads limit the size of their trains, which can routinely stretch more than 2 miles long. However, they did suggest a number of precautions including making sure engineers know how to handle them and that locomotives don't lose communication with devices at the end of trains

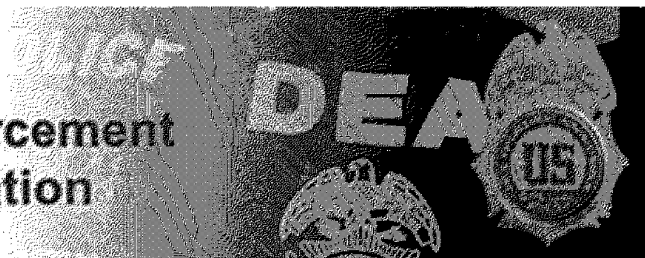
that can help trigger the brakes in an emergency. Currently, there aren't any restrictions on train length but members of Congress and state lawmakers in at least six states have proposed establishing limits particularly in the wake of the fiery Feb. 3 Norfolk Southern derailment in Ohio. Source; Manufacturing.com, 5/1/2023

Analyst Comment On 27 April, the Federal Railroad Administration (FRA) issued a safety advisory regarding "long trains," warning "railroads and railroad employees to be particularly mindful of the complexities of operating longer trains" in the wake of recent derailments. In the advisory, the FRA cites three examples of recent derailments that were caused by trains over 12,250 feet (3,734 meters), where train length played a role in the cause of the derailments. The derailments mentioned as examples were in Springfield, Ohio in March 2023; in Ravenna, Ohio in November 2022; and in Rockwell, Iowa in March 2022. In each of those cases, the FRA said "the way cars in different parts of the train pulled and pushed against each other contributed to the derailments." This latest advisory follows an advisory from earlier this month that directed railroads to reexamine the way they assemble their trains to minimize those kinds of forces, which often come into play as a train goes over hills and around corners. In addition to the concerns about derailments, long trains can block crossings for extended periods of time, which the U.S. Government Accountability Office (GAO) says can impede emergency responders and prompt "unsafe pedestrian behavior (such as climbing through stopped trains)." The states proposing limits on train size this year include Arizona, Iowa, Kansas, Michigan, Nevada and Washington. Source; Surface Transportation & Public Transportation ISAC Transit & Rail Intelligence Awareness Daily Report (TRIAD)

INTERNATIONAL



**U.S.
Drug Enforcement
Administration**



DEA Operation Last Mile Tracks Down Sinaloa and Jalisco Cartel Associates Operating within the United States

Reveals That Social Media Platforms Play Significant Role in Cartels' Ability to Get Fentanyl and Methamphetamine into American Communities

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****

WASHINGTON – Today, the U.S. Drug Enforcement Administration announced the results of a year-long national operation, “Operation Last Mile,” targeting operatives, associates, and distributors affiliated with the Sinaloa and Jalisco Cartels responsible for the last mile of fentanyl and methamphetamine distribution on our streets and on social media.

DEA’s top operational priority is to defeat the Sinaloa and Jalisco Cartels—the two drug cartels based in Mexico that are responsible for the vast majority of the fentanyl and methamphetamine that is killing Americans. In Operation Last Mile, DEA tracked down distribution networks across the United States that are connected to the Sinaloa and Jalisco Cartels. The Operation shows that the Sinaloa and Jalisco Cartels use violent local street gangs and criminal groups and individuals across the United States to flood American communities with huge amounts of fentanyl and methamphetamine, which drives addiction and violence and kills Americans. It also shows that the Cartels, their members, and their associates use social media applications—like Facebook, Instagram, TikTok, and Snapchat—and encrypted platforms—like WhatsApp, Telegram, Signal, Wire, and Wickr—to coordinate logistics and reach out to victims.

Operation Last Mile comprised 1,436 investigations conducted from May 1, 2022 through May 1, 2023, in collaboration with federal, state and local law enforcement partners, and resulted in 3,337 arrests and the seizure of nearly 44 million fentanyl pills, more than 6,500 pounds of fentanyl powder, more than 91,000 pounds of methamphetamine, 8,497 firearms, and more than \$100 million. The fentanyl powder and pill seizures equate to nearly 193 million deadly doses of fentanyl removed from communities across the United States, which have prevented countless potential drug poisoning deaths. Among these investigations, more than 1,100 cases involved social media applications and encrypted communications platforms, including Facebook, Instagram, TikTok, Snapchat, WhatsApp, Telegram, Signal, Wire, and Wickr.

“The Sinaloa and Jalisco Cartels use multi-city distribution networks, violent local street gangs, and individual dealers across the United States to flood American communities with fentanyl and methamphetamine, drive addiction, fuel violence, and kill Americans,” said Administrator Milgram. “What is also alarming—American social media platforms are the means by which they do so. The Cartels use social media and encrypted platforms to run their operations and reach out to victims, and when their product kills Americans, they simply move on to try to victimize the millions of other Americans who are social media users.”

“As our communities continue to grapple with drug poisonings, the sales of illicit drugs, and the violence that so often accompanies these crimes, our local, state, and federal partnerships have never been more important,” said Eddie Garcia, President of the Major Cities Chiefs Association. “Working together and towards the same goal has paid dividends when it comes to impacting criminal networks that continue to seek death and destruction on our streets.”

“Arrests focusing on key components of the drug cartel’s illegal drug distribution chain will help all of us in our efforts to disrupt and dismantle criminal organizations who are flooding our nation with deadly drugs and violence,” said Sheriff Mike Minstead, Chair of the Drug Enforcement Committee, National Sheriffs’ Association. “The strategy of DEA to coordinate these investigations with state/local/tribal law enforcement agencies has once again proven effective and we applaud the results of this nationwide investigation.”

“The Major County Sheriffs of America (MCSA) commends the Drug Enforcement Administration for their efforts during Operation Last Mile. The MCSA is proud to stand alongside our partners at the DEA to end this crisis and protect our citizens from the cartels,” said Sheriff Dennis Lemma, MCSA President. “The results of this yearlong investigation are unprecedented and demonstrate the importance of federal, state, and local law enforcement agencies working together.”

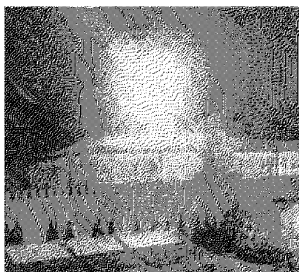
Operation Last Mile is an example of DEA’s network-based approach to take out Sinaloa and Jalisco Cartel members and associates in the United States and across the globe, stop fentanyl, and save American lives. In April 2023, the DEA and our federal partners announced the indictment of 28 members and associates of the Sinaloa Cartel operating in Mexico, China, and Central America, including the leaders of the Cartel known as the “Chapitos.” Source: DEA

Analyst Comment In Portland, Oregon – On Wednesday, a Mexican national with ties to the Sinaloa Drug Cartel was sentenced to 26-years in prison for conspiracy to commit kidnapping resulting in death, conspiracy to possess drugs with intent to distribute and for illegally re-entering the US twice following prior removals. The subject denied involvement in

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****

the kidnapping and murder of the victim but admitted to keeping watch over him for several days, as he was beat to death and then transferring the victim's body to a roadway. The subject did not identify others involved, afraid that he and his family in Mexico could be killed.

Kremlin Drone Attack



Drone attack on Kremlin

On Wednesday, at 2:30 a.m. a pair of explosions over the Kremlin were recorded on video, most likely delivered by unmanned aerial vehicles, reported the NYT. There were no reports of serious damage or casualties but the attack has generated wild speculation about the source and ominous threats from the Russian government. The Ukrainian government has officially denied involvement, but the Russian spokesman has characterized the attack as terrorism and has blamed the US for orchestrating the operation.

Analyst Assessment The attack on the Kremlin has increased fears of Russian retaliation and escalation aimed at Ukraine, the US, and western allies. Pro-Putin hardliners have been pushing for major escalations; from calling for the assassination of the Ukrainian President, to the use of nuclear weapons. The Institute for the Study of War believes the attack is most likely a false flag operation, staged to further Russian political agendas. Currently, the Russians are expecting a Ukrainian offensive. Russian cyber activity, election interference, and disinformation campaigns will likely continue or accelerate against the US and western targets. Source; Watchline@fdny.nyc.gov

Other National/International Articles of Interest (Links):

FBI Warrantless Searches of Americans' Data Plummet in 2022, Intel Report Says

<https://www.cnn.com/2023/04/28/politics/fbi-americans-data-intelligence-report/index.html>

More People Are Getting Away with Murder, Unsolved Killings Reach a Record High

<https://www.npr.org/2023/04/29/1172775448/people-murder-unsolved-killings-record-high>

Frequent Shootings Put U.S. Mass Killings on a Record Pace

<https://apnews.com/article/mass-killings-record-pace-2023-d685a6cd67e0f449f3f9d1d8713d451c>

Nearly a third of nurses nationwide say they are likely to leave the profession

<https://www.npr.org/2023/05/02/1173107527/nursing-staffing-crisis>

Three Men Arrested in Child Sex Sting During NFL 2023 Draft in Kansas City

<https://news.yahoo.com/three-men-arrested-child-sex-205625475.html>

Top Gulf drug cartel lieutenant Hugo Salinas Cortinas, dubbed 'The Goat,' arrested near Texas border

<https://nypost.com/2023/05/02/top-gulf-drug-cartel-lieutenant-dubbed-the-goat-arrested/>

TSA is rolling out a new facial recognition technology to check IDs at airports across the country

<https://www.businessinsider.com/tsa-facial-recognition-technology-airports-credential-authentication-cat-baltimore-washington-2023-5>

Report: LEOs shot in ambush-style attacks increases 10% over last year

<https://www.police1.com/officer-safety/articles/report-leos-shot-in-ambush-style-attacks-increases-10-over-last-year-qW0RCWkjYAO2m733/>

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****

Cameras, LPRs help officers track, locate and arrest Atlanta gunman

https://www.police1.com/police-products/traffic-enforcement/license-plate-readers/articles/cameras-lprs-help-officers-track-locate-and-arrest-atlanta-gunman-hT0pcvGq1Z9VmNSm/?utm_source=Police1&utm_campaign=a01df92856-EMAIL_CAMPAIGN_2023_05_04_05_53&utm_medium=email&utm_term=0_5584e6920b-3877e91294-%5B%5D

United States: California to Start Phase Out All Diesel Trucks at Ports Next Year

<https://www.maritime-executive.com/article/california-to-start-phase-out-all-diesel-trucks-at-ports-next-year>

The post-Title 42 border surge has already begun

<https://www.nbcnews.com/politics/immigration/title-42-border-surge-already-begun-rcna82980>

Georgia Is Using a Domestic Terrorism Law Expanded After Dylann Roof Against ‘Cop City’ Protesters

<https://time.com/6276994/georgia-domestic-terrorism-law-cop-city/>

Belgian Police Arrest Seven People Over Terror Attack Plot

<https://www.theguardian.com/world/2023/may/04/belgian-police-arrest-seven-islamic-state-terror-attack-plot>

UK police well prepared for King Charles's coronation

https://www.reuters.com/world/uk/uk-prepared-security-challenge-king-charles-coronation-minister-2023-05-03/?utm_source=Sailthru&utm_medium=Newsletter&utm_campaign=Daily-Briefing&utm_term=050523

*TPD/PCSD Homeland Security Reports Received this week 7.

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****