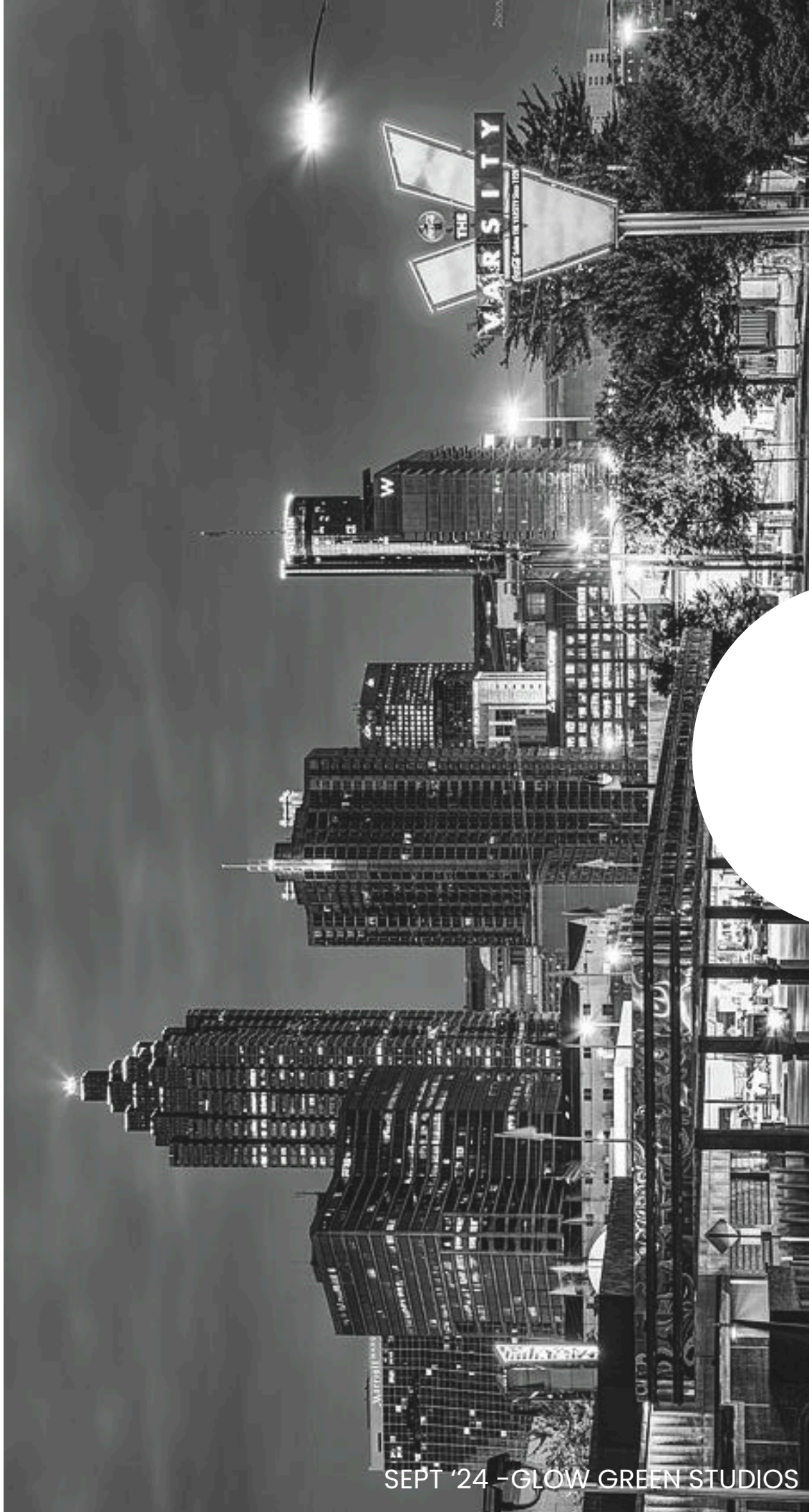


BRIEFING

OFFICE OF INVESTIGATIVE AID



SEPT '24 - GLOW GREEN STUDIOS

HOMELAND SECURITY

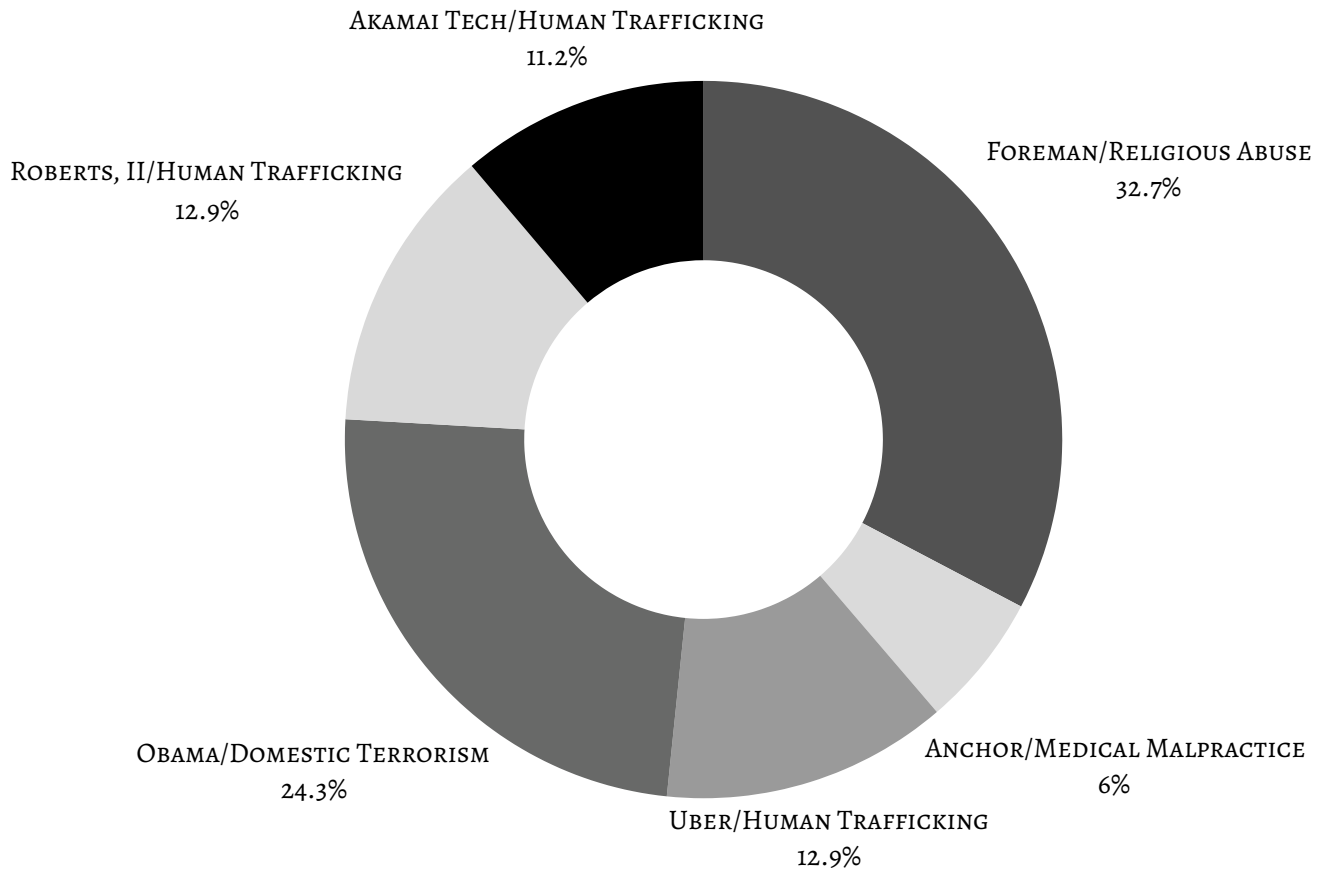
According to the 2024 Homeland Security Threat Assessment, “In 2024, we expect the threat of violence from violent extremists radicalized in the United States will remain high but largely unchanged from the threat as described in the May 2023 National Threat Advisory System (NTAS) bulletin. Over the past year, both domestic violent extremists (DVEs) and homegrown violent extremists (HVEs) inspired by foreign terrorist organizations have engaged in violence in reaction to sociopolitical events. These actors will continue to be inspired and motivated by a mix of conspiracy theories; personalized grievances; and enduring racial, ethnic, religious, and anti-government ideologies, often shared online.

- Since January 2022, DVEs have conducted three fatal attacks in the Homeland resulting in 21 deaths and multiple non-lethal attacks. US law enforcement has disrupted over a half dozen other DVE plots. During the same period, only one attack was conducted by an individual inspired by a foreign terrorist organization. The individual—who is awaiting trial—was likely inspired by a spiritual mentor of al-Qa’ida and Taliban narratives and allegedly wounded three New York City Police Department officers on New Year’s Eve.
- Collectively, these incidents focused on a variety of targets, including law enforcement, government, faith-based organizations, retail locations, ethnic and religious minorities, healthcare infrastructure, transportation, and the energy sector. The most lethal attack this year occurred in May in Allen, Texas, where a now-deceased attacker killed eight people at a shopping mall. The attacker was fixated on mass violence and held views consistent with racially or ethnically motivated violent extremist (RMVE) and involuntary celibate violent extremist ideologies, judging from his writings and online activities.
- While violent extremists likely will continue using accessible, easy-to-use weapons for attacks, they also will leverage online platforms and encrypted communications applications to share novel tactics and techniques. Collaboration among violent extremists online likely will grow as they strive to spread their views, recruit followers, and inspire attacks. Some RMVEs have improved the quality of their video and magazine publications online, which could help them inspire more like-minded individuals to commit attacks.” (DHS 2024 Threat Assessment: Terrorism – Page 3)

“Malicious cyber actors have begun testing the capabilities of AI-developed malware and AI-assisted software development—technologies that have the potential to enable larger scale, faster, efficient, and more evasive cyber attacks—against targets, including pipelines, railways, and other US critical infrastructure. Adversarial governments, most notably the PRC, are developing other AI technologies that could undermine US cyber defenses, including generative AI programs that support malicious activity such as malware attacks.” (DHS 2024 Threat Assessment: Terrorism – Page 18)

“Some DVEs, particularly those motivated by conspiracy theories and anti-government or partisan grievances, may seek to disrupt electoral processes. Violence or threats could be directed at government officials, voters, and elections-related personnel and infrastructure, including polling places, ballot drop box locations, voter registration sites, campaign events, political party offices, and vote counting sites.” (DHS 2024 Threat Assessment: Terrorism – Page 19)

GGs [MMTS DOMESTIC TERRORISM] THREAT ANALYSIS



The MMTS is an act of domestic terrorism. The highly illegal operation involves corrupt organizations, corrupt officials, and organized gang activity. The AI driven human trafficking conspiracy targets and attacks citizens of the United States with intentions to exploit sensitive information for economical gain, extreme political ideologies, and religious agendas. The homegrown pursuit bares the burden of revealing the criminalization of poverty and Mass Incarceration. *The United States Department of State defined terrorism in 2003 as "premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience."* https://en.wikipedia.org/wiki/Domestic_terrorism

On June 27, 2023, the Biden-Harris Administration issued a fact sheet for the "[National Strategy for Countering Domestic Terrorism Strategic Implementation Update](#)." In order to **Prevent Domestic Terrorism Recruitment and Mobilization**, the administration suggested strategies which includes the "expanding of community-based diversion of individuals at risk of committing targeted violence or terrorism" and "addressing the role of the Internet in influencing individuals to commit acts of domestic terrorism." In regard to **Disrupting and Deterring Domestic Terrorism**, its best to "prioritize domestic terrorism-related investigations and prosecutions at both the national and local level."

1. **Mass Manipulation Trafficking Scheme (MMTS):** is a conspiracy to gain unauthorized access to digital devices and mobile applications to track, traffic, and coerce a targeted individual.
2. **Corruption:** is a dishonest, fraudulent, or even criminal act of an individual or organization, using entrusted authority or power to make a personal gain or other unethical or illegal benefits.
3. **Domestic Terrorism:** or homegrown terrorism is a form of terrorism in which victims "within a country are targeted by a perpetrator with the same citizenship" as the victims. The Patriot Act defines domestic terrorism as an attempt to "intimidate or coerce a civilian population; to influence the policy of a government by intimidation or coercion; or to affect the conduct of a government by mass destruction, assassination, or kidnapping."

CORRUPTION

Sad to say, in context of the MMTS, corruption played a part in the conspirators attempt to delay judicial proceedings by misinforming novice government employees within the Armed Forces, the FBI, Police Departments and District Courts. The corrupt bureaucrat and associates influenced the naive agents, deputies, etc into making decisions on their behalf by manipulating religious or political beliefs. Zoning in on extremism in the military, in 2021, Secretary of Defense Lloyd Allen cited at The Pentagon that extremism is not new to the country or new to the military. What is new is how fast extreme ideology can travel through social media and how many hate groups and sympathizers are applying social media to their operation. Allen stated that *"we can't afford action and behavior that are at odds with our values and that undermine good order and discipline that harm or harass and otherwise violate the oath that we share and the bonds of trust that which we all rely."*

Corruption is an act of domestic terrorism when in attempt to sway the government, citing the Inspector General of Georgia. On June 03, 2021, the Biden-Harris Administration issued a fact sheet for "Establishing the Fight Against Corruption as a Core U.S. National Security Interest". The fact sheet addresses that *"corruption threatens U.S. national security by eroding citizens' faith in government, distorting economies, and enabling authoritarians to weaken democratic institutions. The Biden-Harris Administration is committed to taking new steps to hold accountable corrupt individuals, transnational criminal organizations, and other actors engaged in illicit activity."* Starting the simple process for relief resulted in an initiation of insurrection and racketeering charges, including but not limited to retaliation against a victim or witness, the attempt to tamper with a victim, obstruction of justice, and obstruction of a criminal investigation. Domestic Terrorism for the FBI's purposes is referenced in Title 18 Section 2331(5), and is defined as activities: Involving acts dangerous to human life that are a violation of the criminal laws of the United States or of any State.

MASS MANIPULATION TRAFFICKING SCHEME

Developer software like Bonjour, Open AI, and Fing has left a bad taste in the mouth of electronic enthusiasts who enjoy Apple, Android, Samsung, and HP products on a consumer level. Without permission, Foreman was able to use Fing to find all available devices on a network, and Bonjour & other spyware programming to seamlessly install various multicast services within Jas Lundie's computer. Although its impossible to remove the background services from the administrator, the command prompt application allows GGs Office of Threat Intelligence to locate the connection via "netstat - ano."

```
[fe80::7a1f:43f7:67f6:5%16]:1900  *: * 15720
[fe80::7a1f:43f7:67f6:5%16]:63952 *: * 15720
```

FIG1

The Man-In-The-Middle attack is how the co-conspirators are gaining unauthorized access to digital devices and mobile applications. *"The attacker gains access to a private communications channel in some form. The methods of gaining access may include intercepting network traffic, hacking into an unsecured Wi-Fi hotspot, or exploiting vulnerabilities in web applications. There are many different types of man-in-the-middle attacks, making it essential for businesses to recognize all the warning signs. Security researchers have discovered potential MITM attacks targeting Internet routers, real-time locating system (RLTS) technology, and even smartwatches for children. Attackers may hack into unsecured Wi-Fi networks or set up a malicious Wi-Fi hotspot to view users' communications. For example, an attacker may establish a Wi-Fi hotspot with the name of a nearby business, tricking users into connecting."* <https://www.eccouncil.org/> Due to Foreman sharing the electronic serial number of Jas Lundie's access device, RICO violation, Akamai Tech was able to latch on to the plaintiff's laptop illegally. We were able to locate by utilizing the cmd "nslookup {ip address}" in the powershell.

```
PS C:\Users\Jas> nslookup 104.76.210.212
Server:      cdns01.comcast.net
Address:     2001:558:feed::1

Name:   a104-76-210-212.deploy.static.akamaitechnologies.com
Address: 104.76.210.212
```

FIG 2

By instruction of a conspirator, the company has integrated all browsers into a larger Artificial Intelligence machine funded by advertisers and leading tech giants, for example Google. In attempt to obstruct justice vulnerabilities within sites are exploited to prevent communication with organizations that could advocate for the plaintiff's relief. Emails are spiraling into the spyware portal, disguised as a group chat, and by analyzing the data within the security systems, we were able to locate 227 threat actors attacking the host of the domain. The attack is stemming from Akamai's integration.



Profile	Country/region of origin	Targets	Defender TI indicators
 Aliases: Volatile Cedar Amethyst Rain is Microsoft's name for a Lebanon-based actor assessed to have ties to Lebanese Hezbollah. Amethyst Rain primarily targets organizations in the healthcare, government, legal, shipping, and transportation sectors based in, or with ties to, Israel. In past operations, Amethyst Rain operators have primarily exploited vulnerabilities in internet-facing appliances...	 Lebanon	<ul style="list-style-type: none">Government Agencies & ServicesHealthcare & Public HealthTransportation Systems: Postal and Shipping	0

FIG 3

On October 30, 2023, the Biden Administration issued an Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. It states that, "Artificial Intelligence policies must be consistent with my Administration's dedication to advancing equity and civil rights. My Administration cannot – and will not – tolerate the use of AI to disadvantage those who are already too often denied equal opportunity and justice. My Administration will build on the important steps that have already been taken – such as issuing the Blueprint for an AI Bill of Rights, the AI Risk Management Framework, and Executive Order 14091 of February 16, 2023 (Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government) – in seeking to ensure that AI complies with all Federal laws....civil liberties, equity, and justice for all."

NEUTRAL AMERICAN IN A TIME OF WAR

The Mass Manipulation Trafficking Scheme ignited a civil war: good vs evil, right vs wrong, the aware vs the ignorant, and a series of other debates that's sparking political mayhem. Even though she is the leader of the good that follow her, combatants, the conversations surrounding the 2024 Election and civil laws are placing the victim in neutrality. She has absolutely no interest in discussing the topics on her social media accounts and within her case file but the corruption facilitating the MMTS is placing her in harms way.

The weaponization of the spiritual attachment, the voodoo doll used to torture her, and obstruction of justice shows clear signs of discrimination against neutral Americans in a time of war. Thus, violating Title 15 Section 77. The integration of her phone and laptop, without any financial resources to solve the issues, is displaying how irresponsible these criminals are and could possibly set the stock market to crash. It's within the public interest for the SEC to investigate the technological aspect of the scheme pursuant to Title 15 Section 77t. The operating systems for her devices comes pre-installed with stock market applications and the integration purpose is to manipulate the contents of those apps.

The plaintiff cannot run her company, she has no source of income and the defendant continues to threaten her life if she does not comply or mute her distress. Title 15 Section 77 falls under Subchapter 6, Prevention of Unfair Methods of Competition. Can the court conclude that the domestic terrorism is an unfair method of competition?