2025

Threat Assessment

New Jersey Office of
Homeland Security and Preparedness

njohsp.gov | cyber.nj.gov

About NJOHSP

The New Jersey Office of Homeland Security and Preparedness (NJOHSP) is tasked with coordinating efforts in counterterrorism, counterintelligence, targeted violence prevention, preparedness, and cybersecurity across all levels of government, law enforcement, nonprofit organizations, and the private sector. Created by Executive Order in 2006 when the Office of Counterterrorism (OCT) merged with staff from the Domestic Security Preparedness Task Force (DSPTF), NJOHSP bolsters New Jersey's resources for counterterrorism, critical infrastructure protection, preparedness, training, and federal and State grant management.

Shortly after the tragic events of September 11, 2001, New Jersey's legislature and Governor passed and signed the Domestic Security Preparedness Act, which created the DSPTF within the Office of the Attorney General. In 2002, the Governor created the OCT by Executive Order, which remained under the Attorney General. OCT provided New Jersey with a single agency to lead and coordinate New Jersey's counterterrorism efforts with state, local, and federal authorities and with the private sector.

Mission

To lead and coordinate New Jersey's counterterrorism, counterintelligence, cybersecurity, and preparedness efforts.

Core Values

SERVICE. We put our State and its citizens first, and we put Mission before self. We take pride in being timely, accurate, and relevant.

TEAMWORK. We stand with and behind each other. We recognize that partnerships, both internal and external, are critical to achieving success. We cannot fulfill our Mission alone.

EXCELLENCE. We take great pride in the quality of our work. We do every task, every project, every initiative, to the best of our ability.

DIVERSITY. We strive to build a workforce that is as diverse as New Jersey's citizenry. We pride ourselves on encouraging diversity of thought, perspective, and problem solving.

INTEGRITY. We are committed to holding ourselves accountable to the highest moral and ethical standards in our personal and professional conduct. We can be relied upon to act with honor and truthfulness.

Foreword

The New Jersey Office of Homeland Security and Preparedness (NJOHSP) remains a pivotal authority in safeguarding the state and its residents, visitors, businesses, and various communities. We continue to mitigate risks by implementing proactive security and preparedness strategies, building robust partnerships with federal, State, and local law enforcement, and collaborating with the private sector. NJOHSP remains committed to preventing and countering terrorism, foreign intelligence efforts, and cyber threats, all while consistently evolving with the ever-changing threat landscape.

Moving forward in 2025, NJOHSP analysts assess homegrown violent extremists (HVEs), and white racially motivated extremists as the highest threats to New Jersey. Their dedication and willingness to commit violence remains a persistent threat to the state. This threat was evident on January 1 when Shamsud-din Bahar Jabbar, an HVE and ISIS supporter, drove a rented truck through Bourbon Street in New Orleans during a New Year's celebration, killing 14 individuals and injuring at least 57. These acts of violence continue to highlight the sustained threat from extremists and the importance of remaining prepared and vigilant.

As the world evolves, so do the capabilities of threat actors. Extremists across all ideologies seek to recruit and radicalize individuals and as the use of generative artificial intelligence increases, we also expect extremists to use these new technologies to mass-produce propaganda, create deepfakes, and facilitate real-time interactions.

We are steadfast in our commitment to protecting critical infrastructure—such as energy, financial, healthcare, and telecommunications systems—against the escalating cyber threats posed by advanced persistent threat actors and state-sponsored cybercriminals, who are relentlessly targeting both private- and public-sector entities in New Jersey, using sophisticated cyber tactics to disrupt operations, steal sensitive data, and undermine security. These cyberattacks have the potential to adversely impact public health, the welfare and safety of our residents, the economy and public interests of the State, and national security. This growing cyber threat demands urgent, proactive cybersecurity measures to fortify our defenses and safeguard our critical infrastructure from relentless attacks.

Despite these threats, our dedication to helping ensure the safety and security of our state, its residents, and visitors is of the utmost importance. On behalf of NJOHSP and its staff, I extend our gratitude to all our partners who contributed to our 2025 Threat Assessment, assisting our efforts to meet future challenges, especially as we prepare for significant upcoming events, such as the 2025 FIFA Club World Cup, the 2026 FIFA World Cup, and the 250th anniversary of the U.S. These events will bring together diverse communities and present unique security challenges, and we are committed to ensuring the safety and security of all. As the public serves as one of our most effective first lines of defense against terrorism and threats, I encourage everyone to remain vigilant. If you "See Something, Say Something" by reporting suspicious activity with a nexus to terrorism, targeted violence, or other related activity to NJOHSP's Counter-Threat Watch Unit at 866-4-SAFE-NJ or tips@njohsp.gov.

Sincerely,

Laurie R. Doran
Director
February 2025

Information Cutoff: December 31, 2024

Table of Contents

New Jersey's Assessed Threat Level in 2025

2025 Assessed Threat Level

High	Homegrown Violent Extremists
	White Racially Motivated Extremists
Moderate	Abortion-Related Extremists
	Anarchist/Anti-Fascist Extremists
	Anti-Government Extremists
	Sovereign Citizen Extremists
Low	Al-Qa'ida and Affiliates
	Animal Rights Extremists
	Black Racially Motivated Extremists
	Environmental Extremists
	HAMAS
	Hizballah
	ISIS
	Militia Extremists

Detailed information on these extremist groups and individuals can be found at njohsp.gov/threat-landscape/domestic-threats and njohsp.gov/threat-landscape/foreign-terrorist-organizations.

Changes from 2024

The threat from Black Racially Motivated Extremists and Militia Extremists in New Jersey decreased from moderate to low in 2025.

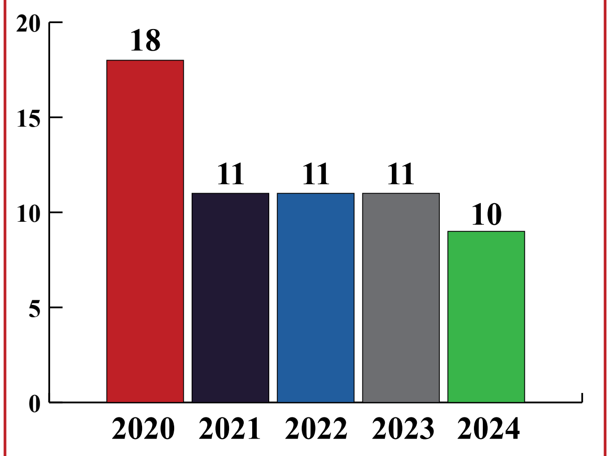
Anarchist/Anti-Fascist Extremists: This threat category was updated to include the actions of individuals and groups that oppose "oppressive" governments, laws, and law enforcement officers.

High Threats in 2025

HVEs Look to ISIS for Inspiration to Commit Violence

Homegrown violent extremists (HVEs) will find ISIS to be the most appealing foreign terrorist organization (FTO) to support, seeking to travel and join the group, provide it monetary support, and commit attacks on its behalf, despite the recent popularity of other FTOs. Since the October 7, 2023, HAMAS attack on Israel, ISIS remains the primary motivator of HVEs in the U.S. despite the increased popularity and media coverage of groups such as HAMAS and Hizballah. An NJOHSP review of HVE incidents since 2015 found that 75% of individuals supported ISIS as opposed to other FTOs.

Identified HVEs by Year*



**Due to the sensitivity of criminal investigations, this data only reflects publicly available information and may be subject to change.*

In October 2024, authorities arrested Michael Teekaye, Jr., of Maryland, for attempting to travel to join ISIS. Teekaye communicated online with an undercover officer and expressed his desire to travel to Africa and fight for ISIS. He claimed he was in contact with an ISIS fighter who was assisting him and, if he could not travel, his "plan B" was to attack individuals in the U.S. who supported Israel. Teekaye purchased ammunition, reserved time at a shooting range, and attempted to purchase a rifle but was denied since he was on probation due to an unrelated state-level criminal case. A few days prior to his arrest, Teekaye confirmed he was willing to join ISIS, claimed he conducted research, and said that the group is the only one "that has the most true and sincere intentions."

In May 2024, federal authorities arrested Jibreel Pratt in Detroit after he sent money to ISIS and desired to travel in support of the group. In February 2023, Pratt initiated contact with a federal informant whom he thought was an ISIS travel facilitator. Pratt expressed his support for ISIS and his desire to travel overseas to join the group and become an ISIS leader. Pratt sent money to the group via Bitcoin between March 2023 and May 2024. Pratt continued to communicate with the informant and drafted plans to use explosives to kill, kidnap, or sabotage and create an intelligence unit for ISIS. Although Pratt was prohibited from purchasing firearms per the bond conditions of a separate federal case against him involving financial fraud, law enforcement officials alleged he still acquired several firearms, ammunition, and combat gear.

In April 2024, authorities arrested Alexander Mercurio, of Idaho, for providing material support to ISIS. Mercurio planned to incapacitate his father, steal his firearms, and then conduct a suicide attack at a local church. Mercurio consumed and spread ISIS propaganda online and discussed traveling overseas to join the group. Mercurio used a school-issued laptop to engage with like-minded individuals via encrypted messaging platforms and discussed supporting ISIS to possibly commit an attack. Mercurio claimed his radicalization began during the COVID pandemic, and that he previously "drank the Kool-Aid" of white racially motivated extremism; however, after discovering ISIS, he felt the group held "more purpose for him." A few days before the date of the planned attack, he filmed a video of himself in front of an ISIS flag pledging allegiance to the group.

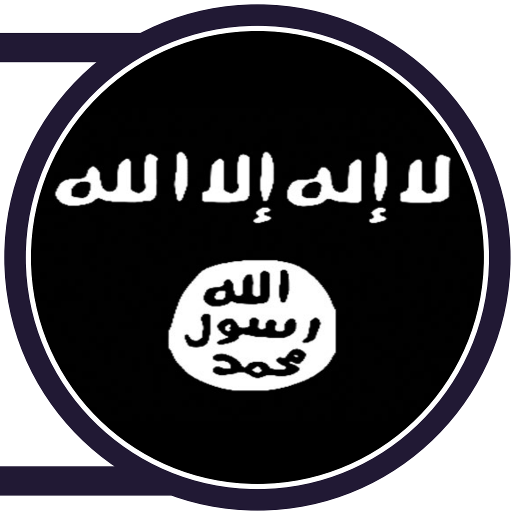
HVEs: 2024 Regional Arrests

Mohamad Hamad | **Coraopolis, Pennsylvania**

In October 2024, law enforcement officials arrested Mohamad Hamad on hate crime charges after he and another co-conspirator vandalized Jewish buildings in the Pittsburgh area. Hamad called himself a "self-described HAMAS operative" due to his hatred of Israel and the Jewish community and his desire to "die a martyr for Islam." Hamad purchased explosive materials online and communicated with another individual through an encrypted messaging platform about wanting to build an explosive device and initiating a test detonation in July 2024.

Syed Aman | **Franklin Square, New York**

In November 2024, authorities charged Syed Aman with material support after he attempted to board a plane at New York's JFK International Airport to join ISIS in Syria. According to the criminal complaint, throughout 2023 and 2024, Aman used social media to express his support for ISIS. He sent money to an individual he believed to be an ISIS operative to facilitate his travel to Syria to join the group. Aman also posted on social media his desire to "kill Americans" and wrote in a notebook that he wanted to be a "martyr on behalf of ISIS."



Jack Molloy | **Upper St. Clair, Pennsylvania**

In December 2024, law enforcement officials arrested Jack Molloy for making false statements regarding his involvement with a foreign terrorist organization. Molloy traveled to Lebanon in August 2024 to join Hizballah. After encountering difficulties joining the group, Molloy traveled to Syria in October 2024 to join the group's Syrian branch. According to the Department of Justice, after Molloy's return to the U.S., he denied his involvement with the group. Officials reported that Molloy "continued to engage in conduct consistent with his desire to join Hizballah" and that he "supported and idolized violence and wanted to kill Jews."

WRMEs Embrace Varied Plots and Threats

White racially motivated extremists (WRMEs) will engage with supporters both online and in person to bolster training and recruitment efforts along with encouraging others to commit attacks to further their ideology. Over the past year, WRMEs primarily focused on threats and plots to attack their perceived enemies while trying to attend in-person gatherings to garner attention.

Patriot Front members demonstrate near the Tennessee House of Representatives and State Capitol.

In July 2024, authorities arrested Andrew Takhistov, of East Brunswick (Middlesex County), for plotting an attack on electrical substations in New Jersey to further his WRME ideology. Takhistov utilized numerous social media platforms to express his desire to commit an attack while praising past shooters such as Brenton Tarrant, the 2019 Christchurch, New Zealand, mosque attacker. On numerous occasions, he communicated with an undercover law enforcement official, both online and in-person, and voiced his intent to travel overseas to join the Russian Volunteer Corps (RVC). He chose the group because it is openly "National Socialist" and specializes in "assassinations, attacks on power grids, and other infrastructure sabotage." Takhistov said he intended to receive extensive training, fight alongside the RVC for a period of time, and bring his experience back to the U.S. He advised the undercover official to research potential targets while trying to recruit and radicalize members to his group to conduct militant activism.

In September 2024, authorities charged Dallas Humber, of California, and Matthew Allison, of Idaho, for leading "Terrorgram," a collection of WRME transnational channels on the encrypted messaging platform, Telegram. The pair adhered to accelerationism, a mainstream WRME ideology, that believes Western governments are corrupt and their demise should be accelerated to create radical social change and a white ethnostate. Humber and Allison actively spread videos and publications called *The Hard Reset*, *White Terror*, and *The List*, provided guidance to commit crimes, celebrated previous WRME attacks, and provided a hit list of "high-value targets" for assassination. The attack list focused on individuals and groups whom the group viewed as "perpetuating an irredeemable society," including U.S. federal, state, and local officials, leaders of private companies, and non-governmental organizations deemed enemies of the white race. The list also encouraged attacks on government infrastructure to aid in societal collapse.

In addition to their online activities, WRMEs have participated in numerous in-person activities including marches, demonstrations, "fight nights," and other propaganda campaigns to garner attention and exploit current issues to fuel their personal grievances. In July 2024, Patriot Front, a white nationalist group, marched the streets of Nashville, Tennessee, with approximately 200 participants allegedly chanting "Sieg Heil" and "Deportation saves the nation," making it one of the largest events for the summer. Goyim Defense League, an antisemitic neo-Nazi group, also protested in Nashville, disrupted a city council meeting, and assaulted a bar employee using a metal flagpole with a swastika attached to the top. In August 2024, members affiliated with a network of active clubs and Patriot Front participated in a Jiu-Jitsu tournament organized by a gym associated with Wolves of Vinland (WOV), a Virginia-based WRME group. Later in the month, the SoCal Active Club, a California-based organization, hosted its third annual "Frontier" fight night, which attracted members from Patriot Front and numerous regional active clubs. Both WOV and SoCal Active Club adhere to the WRME ideology.

Domestic Terrorism

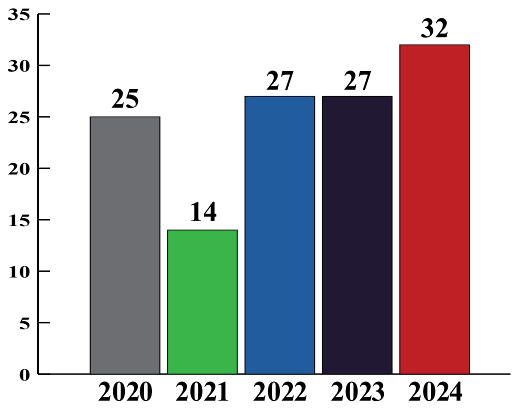
Domestic Terrorism Overview

In 2024, 29 domestic extremists worked independently while three plotted with a co-conspirator to further their ideology. These 35 extremists conducted 32 incidents, including nine attacks, nine plots, and 14 threats. More than half of all incidents targeted the government sector and first responders, including politicians, judges, and law enforcement officers.

In 2024, three unrelated incidents involved two co-conspirators working together to advance their extremist ideologies. In October 2024, authorities arrested Christopher Legere and Cara Mitrano in Pennsylvania on felony eco-terrorism charges. In September 2024, authorities charged Dallas Humber, of California, and Matthew Allison, of Idaho, who were affiliated with an online white racially motivated extremist (WRME) collective, with having a hit list of "high value targets" for assassination that included U.S. federal, state, and local officials. In January 2024, authorities arrested Andrew and Angelo Hatziagelis in Queens, New York, after officials discovered various weapons, improvised explosive devices (IEDs), and ghost guns in their residence. During a search of their home, officials found anarchist propaganda and a hit list containing the names of law enforcement and government officials.

In 2024, extremists with differing ideologies sought to threaten the government sector and first responders through various methods of attack. In April 2024, authorities arrested Kyle Calvert for detonating an IED filled with nails outside the Alabama Attorney General's Office. Calvert placed stickers on various state buildings with phrases to include "Support your antifa." In February 2024, authorities arrested John Mazurek for conducting an arson attack in 2023, that damaged eight police motorcycles. Local authorities linked the attack to extremists protesting the construction of Atlanta's police training center. In three unrelated incidents a self-identified sovereign citizen extremist in Florida and two in Texas resisted arrest and shot at law enforcement officers. During one of the attacks in Texas a sovereign citizen extremist killed a law enforcement officer and injured two others.

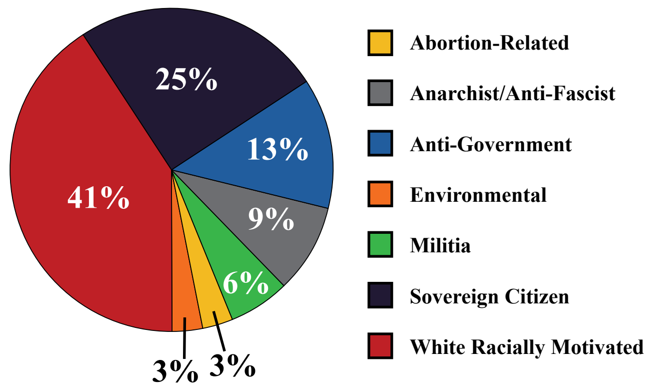
Incidents by Year*



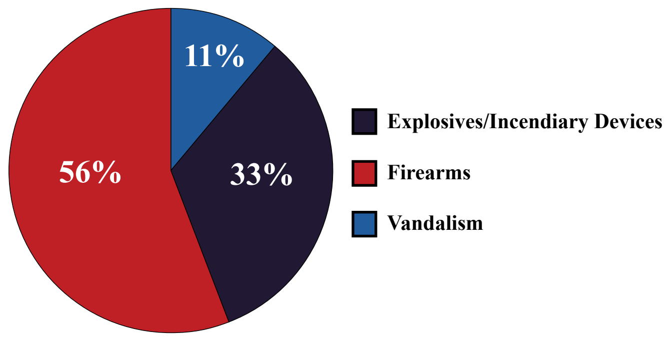
This data only reflects publicly available information related to domestic terrorism incidents nationally and may be subject to change.

Domestic terrorism is violence committed by individuals or groups primarily associated with U.S.-based movements, including anti-government, racially motivated, religious, and single-issue extremist ideologies.

Extremist Ideological Affiliation



Methods Used in Attacks



2024 Domestic Extremism Attack Timeline

February 24

Anarchist/Anti-Fascist Extremist: Kyle Calvert detonated an improvised explosive device (IED) filled with nails and screws outside the Alabama Attorney General's Office. Calvert previously posted anti-fascist (Antifa) content on social media and "expressed his belief that violence should be directed against the government."

March 8

Sovereign Citizen Extremist: Geronimo Kee shot a Memphis law enforcement officer four times during a traffic stop. Kee refused to sign the officer's citation for speeding and said several times that, "You're going to have to kill me." While in court, Kee said, "I am a natural man, created by Yahweh and subject to natural law. Let the record show that."

April 14

Sovereign Citizen Extremist: Patrick Hurst left the scene of a traffic stop and shot at Harris County law enforcement officers in Houston after they deployed spike strips to disable his vehicle. Officers killed Hurst when he exited his vehicle with a handgun to confront them. They initially pulled him over for a damaged tailgate and an expired registration.

April 27

Sovereign Citizen Extremist: Kyran Caples shot and injured two Polk County deputies in Florida after they approached his vehicle in a public park due to burglary concerns in the area. Officers killed Caples after he shot at them and refused to comply with the deputies' orders.

2024 Domestic Extremism Attack Timeline

June 1

Anarchist/Anti-Fascist Extremist: Casey Goonan assembled a bag of six Molotov cocktails and ignited it underneath the fuel tank of an unoccupied University of California Police Department patrol car, damaging it.

August 29

Sovereign Citizen Extremist: Corey Cobb-Bey fatally shot a Dallas law enforcement officer after he approached the police vehicle and engaged in a brief conversation. After fleeing the scene and leading responding officers on a car chase, Cobb-Bey shot and wounded two other officers before being killed.

September 25

Anti-Government Extremist: Nathaniel McGuire injured five individuals after he threw a bag containing an IED inside the lobby of the Santa Barbara County Superior Court, in Santa Maria, California. Law enforcement officers apprehended McGuire as he attempted to enter his parked vehicle. He allegedly yelled that the "government had taken his guns and that everyone needed to fight, rise up, and rebel."

October 22

Anti-Government Extremist: Jeffrey Kelly shot at a Democratic Party campaign office in Arizona three separate times and left bags of white powder labeled as poison near political signs. Authorities discovered more than 120 firearms during a search of his home.

Domestic Extremists Threaten Law Enforcement

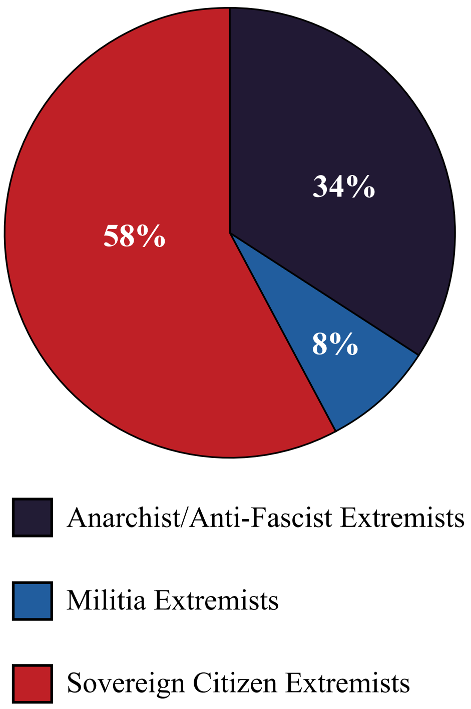
Domestic extremists – primarily anti-government and anarchist/anti-fascist extremists – will reject government authority, laws, and policies, resulting in plots, threats, and attacks against law enforcement officers. In 2024, extremists conducted three plots, three threats, and six planned and opportunistic attacks, using firearms and improvised incendiary devices resulting in one death and five injuries against law enforcement.

In August 2024, Corey Cobb-Bey shot and killed a Dallas police officer in his marked vehicle after engaging in a brief conversation. After fleeing the scene and leading responding officers on a car chase, Cobb-Bey shot and wounded two other officers before being killed. Three days prior to the attack, Cobb-Bey approached an unmarked vehicle, questioned the officer, and posted on social media that an "event" would happen that week. Dallas police said Cobb-Bey made several concerning social media posts and identified as a sovereign citizen.

Various domestic extremists perceive law enforcement as enforcing unconstitutional laws and regulations. Extremists reject their legitimacy to interview, detain, and/or arrest them resulting in deadly confrontations and planned attacks.

In June 2024, Casey Goonan, of California, firebombed an unoccupied University of California Police Department patrol car. According to the indictment, Gonnan ignited and kicked a bag containing six Molotov cocktails underneath the fuel tank of the marked vehicle. Officers initially arrested him on suspicion of possession and use of destructive devices and multiple counts of arson. The criminal complaint referenced a publicly accessible revolutionary movement website that advertised the attack with the headline, "Student Intifada as our Historical Duty: Fulfill it or Betray it." In February 2024, authorities arrested John Mazurek, of Atlanta, for destroying eight police motorcycles in a police parking deck in July 2023. Officials linked this attack, along with two dozen arson attacks, with individuals protesting the construction of an Atlanta-based police training center.

Extremist Attacks and Threats to Law Enforcement in 2024



In February 2024, authorities arrested Paul Faye Sr., of Tennessee, after he attempted to coordinate with militias to attack migrants and federal law enforcement officers at the U.S.-Mexico Border. Faye contacted members of the North Carolina Patriot Party and militias from Kentucky, Georgia, and Tennessee. Faye wanted his actions to inspire others and was in extensive contact with Bryan Perry, of Tennessee, and Jonathan O'Dell, of Missouri, both of whom the FBI arrested in October 2022 at O'Dell's residence. Perry resisted arrest, assaulted one of the officers, and shot at law enforcement vehicles. Perry and O'Dell promoted their plot online and believed border patrol agents who allowed undocumented immigrants into the U.S. committed treason.

Lone Offenders Target High-Ranking Officials

Lone offenders with various personal grievances against national corporations, political parties, and government policies will threaten and conduct attacks targeting high-ranking officials who represent these entities. In 2024, various threat actors and supporters have exploited these incidents to garner attention to their causes and inspire followers to conduct similar attacks.

In December 2024, authorities charged Luigi Mangione for the stalking and murder of UnitedHealthcare CEO Brian Thompson. After engaging in pre-operational planning, Mangione conducted the attack during the morning rush hour outside a New York City hotel. Several days later, authorities arrested Mangione in Pennsylvania and found him with a 9mm pistol and a sound suppressor consistent with the weapon used in the attack. In his handwritten manifesto, Mangione affirmed his dissatisfaction with the healthcare system. Several "wanted" posters and graphics praising the attack circulated online and around New York City in the weeks following his arrest. The incident sparked online conversations among extremists calling for the targeting of additional high profile private- and public-sector executives to further their perceived anti-capitalism and anti-globalism policies.

In November 2024, unknown individuals targeted the homes of six Congressional Democrats from Connecticut and Rhode Island with bombs threats. The previous day, President-elect Donald Trump's transition team reported potential cabinet members and appointees received swatting calls and bomb threats. The investigation into the threats is ongoing. In April 2024, the Department of Justice's Election Threats Task Force opened approximately 100 investigations into threats against election workers, lawmakers, and election officials and charged 20 individuals.

In September 2024, Ryan Routh attempted to assassinate Donald Trump, who was a presidential candidate at the time, at Trump International Golf Club in Florida. While conducting a perimeter security sweep, the Secret Service discovered Routh aiming a rifle at an agent in a tree-covered fenced area. After witnessing the subject move his rifle, an agent opened fire. After fleeing the scene, Routh was later apprehended during a traffic stop. Authorities recovered a semiautomatic rifle with an attached scope and an extended magazine. In July 2024, Thomas Crooks attempted to assassinate Trump at a campaign rally in Butler, Pennsylvania. Trump suffered a non-life-threatening injury while addressing the crowd. Crooks killed one attendee and wounded three others. Secret Service officials returned fire, killing Crooks at the scene. During a search of his vehicle near the site of the rally, authorities recovered two explosive devices from the trunk, and one in Crooks' room at his residence.

Backpack and rifle belonging to Ryan Routh.

Extremists with Varying Ideologies Target Critical Infrastructure

Domestic extremists target a range of critical infrastructure sectors in furtherance of various ideologies to cause widespread disruption of key systems. In 2024, extremists capitalized on divisive social and political issues to fuel their grievances and target critical infrastructure sectors, including government facilities and emergency services, which were the most targeted.

Abortion-Related Extremist **Healthcare and Public Health Sector**	In August 2024, authorities arrested Stephen Gilbert for threatening to attack an abortion clinic in Florida. Gilbert posted to X, “My goal for the week is to find the nearest Abortion Clinic and burn it to the ground #ProLife.” Gilbert was previously convicted of several crimes, including aggravated assault and weapons charges.
Anarchist/ Anti-Fascist Extremist **Government Facilities Sector**	In February 2024, authorities charged Kyle Calvert for his role in detonating an explosive device filled with nails outside of the Alabama Attorney General’s office. According to court documents, Calvert also placed Antifa stickers on buildings in the area, including one that had an Antifa logo and the words “ANTI-FASCISM IS COMMUNITY SELF-DEFENSE,” and “DEATH TO FASCISM.”
Anti-Government Extremist **Government Facilities Sector**	In October 2024, authorities arrested Jeffrey Kelly for shooting at a Democratic National Committee office in Arizona on three separate occasions. In his vehicle, police recovered a grenade launcher, body armor, 120 firearms and 250,000 rounds of ammunition. On his Facebook account, Kelly shared anti-Democrat sentiments, writing that the party is “the TRUE PARTY OF HATE AND DISCRIMINATION.”
Sovereign Citizen Extremist **Emergency Services Sector**	In April 2024, Patrick Hurst shot at law enforcement officers after driving off from a vehicle stop for an expired registration and broken tailgate in Houston. Hurst told the officers that he would not comply with their orders and identified himself as a “sovereign citizen” during his Facebook livestream of the incident.
White Racially Motivated Extremist **Energy: Electric Sector**	In November 2024, authorities arrested Skyler Philippi in Tennessee for plotting to attack interstate electrical substations with a drone. He shared with an undercover law enforcement officer that attacking large substations would “shock the system,” causing other electric substations to malfunction. He also wrote a manifesto expressing his desire to attack “high tax cities or industrial areas.”

NJ Office of Homeland Security and Preparedness

Foreign Terrorist Organizations

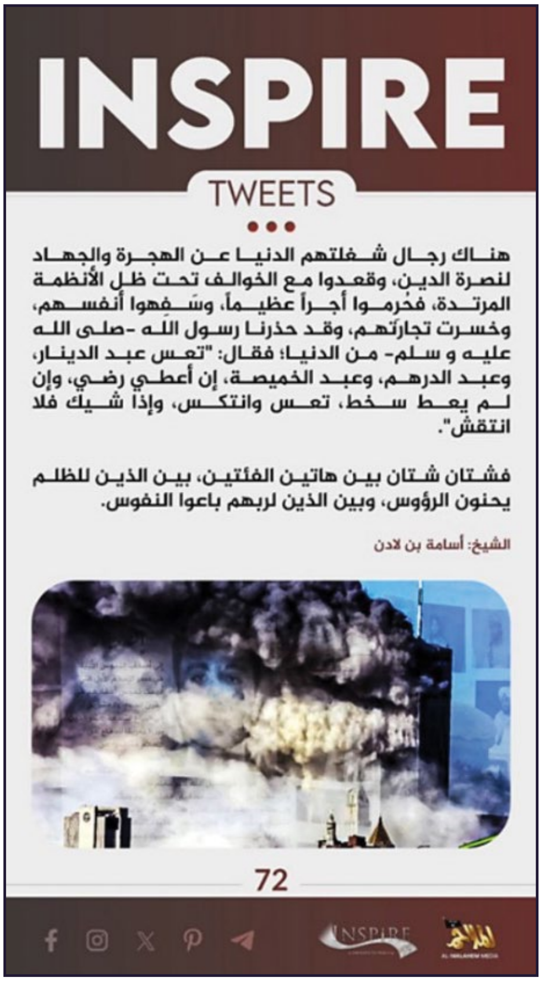
Al-Qa'ida Exploits Global Events to Motivate Supporters

Despite its lack of successful attacks in the West, al-Qa'ida (AQ) exploits global events to motivate supporters by appealing to a sense of duty through encouraging violence, revitalizing propaganda production, and rebuilding its presence in Afghanistan. In a speech in September 2024, National Counterterrorism Center Acting Director Brett Holmgren highlighted how today's threat actors, including AQ's remaining networks, illustrate dangers that are "diverse, decentralized, and complex" and are "often less capable and less sophisticated, but still lethal."

In September 2024, al-Qa'ida in the Arabian Peninsula (AQAP) released a video acknowledging the 23rd anniversary of September 11 and compared it to the October 7, 2023, HAMAS attack on Israel. The group claimed that both events were turning points in history and that those who planned the attacks were fulfilling an "obligatory duty" of "jihad." The video also called for men "in the West… especially in America" to "draw your swords" and attack their enemies. In January 2024, the U.N. released its 33rd Analytical Support and Sanctions Monitoring Team (ASSMT) report stating that AQAP has "significantly reinvigorated its media strategy and content, capitalizing on international events including Qur'an burnings and the 7 October attacks to incite lone actors."

In July 2024, the U.N. released its 34th ASSMT report which stated AQAP had "revitalized its *Inspire* publications, [and was] calling on lone actors to attack in the West." The report claimed the group wants its propaganda to reach a younger audience and is doing so through "brief, appealing '*Inspire* tweets'" and that "the increased use by… al-Qaida groups of the internet and social media for propaganda purposes raises serious concerns for regional states." In addition to *Inspire* tweets, the group also began distributing *Inspire* videos in December 2023, attempting to incite supporters to commit violence in the West and provide operational instructions and possible target ideas.

In June 2024, as-Sahab media, AQ's official media wing, released the third issue of its *This Is Gaza* series, presumably written by AQ leader Saif al-Adel. In the issue, al-Adel draws attention to Afghanistan and encourages those desiring change to "go to Afghanistan, learn from its conditions, and benefit from [the Taliban's] experience." In May 2024, the United States Institute for Peace (USIP) released its final report summarizing counterterrorism in Afghanistan and Pakistan in the wake of the U.S. military withdrawal from Afghanistan in August 2021. It highlighted al-Qa'ida in the Indian Subcontinent (AQIS) as having a presence in the region and discussed how "[AQIS] operates training camps, safehouses, and religious schools in Afghanistan." The report also stated that the Taliban is continuing to support AQ core and that the group's "leadership will retain some type of haven in Afghanistan, which the group could leverage to direct its affiliate network."


INSPIRE
TWEETS
72
INSPIRE

هناك رجال شغلتهم الدنيا عن الهجرة والجهاد لنصرة الدين، وقعدوا مع الخوالف تحت ظل الأنظمة المرتدة، فخرموا أجراً عظيماً، وسَفِهوا أنفسهم، وخسرت تجارتهم، وقد حذرنا رسول الله -صلى الله عليه و سلم- من الدنيا؛ فقال: "تعس عبد الدينار، وعبد الدرهم، وعبد الخميصة، إن أعطي رضي، وإن لم يعط سخط، تعس وانتكس، وإذا شيك فلا انتقش".

فشتان بين هاتين الفئتين، بين الذين للظلم يحنون الرؤوس، وبين الذين لربهم باعوا النفوس.

الشيخ: أسامة بن لادن

AQ propaganda in Arabic.

ISIS Seeks to Achieve Status as Most Competent FTO

ISIS will exert its global reach and external planning capabilities in an attempt to direct and inspire successful attacks in the West and capitalize on its established networks to bolster its image as the most capable foreign terrorist organization (FTO). According to the 2024 Global Terrorism Index, an annual report highlighting global terrorism trends, throughout 2023, ISIS remained the deadliest global FTO in the world, responsible for 1,636 deaths spanning countries in Asia, Europe, Africa, and the Middle East.

In October 2024, the FBI arrested Nasir Tawhedi, an Afghan citizen residing in Oklahoma City, after he planned to purchase two AK-47 assault rifles and 10 magazines which he hoped to use in a mass shooting attack. U.S. officials believe ISIS-Khorasan (ISIS-K), the Afghanistan-based affiliate, directed Tawhedi in his attack planning. Tawhedi allegedly planned to conduct the attack along with his brother-in-law, a juvenile co-conspirator, on Election Day in 2024 to “target large groups of people.” That same week, French authorities arrested an additional family member of Tawhedi’s and two others for plotting an ISIS attack against a soccer stadium or shopping center in France.

In August 2024, a Syrian man identified as “Issa” killed three individuals in a knife attack at a festival in Solingen, Germany. German prosecutors believe Issa “shared the ideology” of ISIS and “joined the group at an undeterminable time.” Following the attack’s success, ISIS-K released an online poster stating, “Don’t underestimate a knife, there is always a way to kill an infidel.” In March 2024, four ISIS-K members attacked Crocus City Hall, a music venue in Moscow, killing 145 people and injuring hundreds more. The attackers used firearms and incendiary devices against the venue and attendees. ISIS claimed direct responsibility for the attack through its Amaq News Agency and shared photos of the attackers.

In 2024, in two separate cases, federal authorities arrested at least nine foreign nationals living in the U.S. for having alleged ties to ISIS. Eight of the individuals are Tajik nationals who lived in Philadelphia, New York City, and Los Angeles. The ninth individual, from Uzbekistan, resided in Baltimore and is awaiting trial in New Jersey. All nine nationals entered the U.S. through the southern border. In June 2024, open-source media reported the U.S. Department of Homeland Security identified at least 400 individuals entered the U.S. using an ISIS-affiliated smuggling network over the last three years. U.S. officials believe there are no indications the individuals plan to carry out terror attacks in the U.S., however, due to the network’s ISIS ties, immigration officials want to arrest them out of “an abundance of caution.”

ISIS Presence in Syria Following Assad’s Overthrow

On December 8, 2024, Syrian rebel forces led by Hayat Tahrir al-Sham (HTS), a former al-Qa’ida affiliate and designated a foreign terrorist organization, successfully seized Syria’s capital, Damascus, and ousted President Bashar al-Assad. HTS leader Abu Mohammad al-Jolani led the group in its overthrow of the Syrian president.

With al-Assad deposed, ISIS may attempt to exploit the current power vacuum in Syria. In 2014, ISIS held large swaths of territory in Syria, allowing it to produce high quality messaging and conduct and inspire terrorism around the world. It maintained a large operational presence in Syria until a global coalition conducted a campaign against the group, removing its grasp in the region. Historically, ISIS has attempted to exploit regions that are in conflict and increase its operational presence, similar to the situation that occurred in Afghanistan following the U.S. withdrawal in 2021. ISIS may view al-Assad’s overthrow as an opportunity to regroup and reconstitute its media output and increase its presence in the country. In response to HTS’s take over, U.S. Central Command announced it carried out more than 75 strikes against ISIS camps and operatives in central Syria to prevent the group from taking advantage of the situation. If ISIS exploits the current situation in Syria, it could reestablish its presence in the region and boost its propaganda efforts, highlighting its operations potentially inspiring HVEs domestically.

NJ Office of Homeland Security and Preparedness

Extremist Use of Social Media

Domestic and Homegrown Violent Extremist Use of Social Media

NJOHSP evaluated 32 domestic extremist attacks, plots, and threats from January 1, 2024, to December 31, 2024. Of the 32 domestic incidents, 19 had a social media nexus. Twenty individuals associated with white racially motivated, anti-government, abortion-related, and anarchist extremist ideologies perpetrated these attacks.

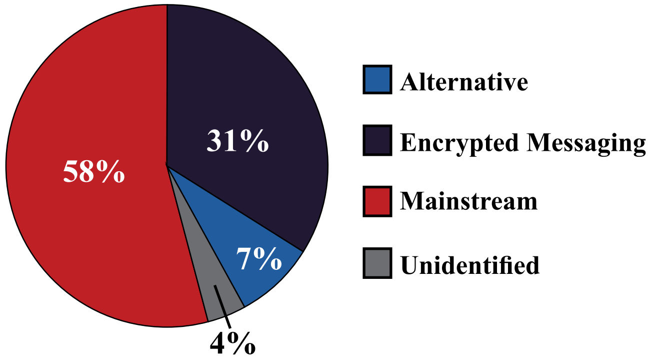
This assessment also identifies trends and patterns of 10 homegrown violent extremists (HVEs) who made threats and provided material support to foreign terrorist organizations (FTOs) from January 1, 2024 to December 31, 2024. All identified HVE cases in 2024 had a social media nexus.

Incidents were collected, reviewed, and analyzed from publicly available sources to create a comparable data set. Chosen parameters included whether a subject had an identifiable extremist ideology, conducted an attack, plot, or threat in furtherance of their ideology, and had a presence on at least one mainstream, alternative, or encrypted messaging social media platform. This data only reflects open-source information related to domestic and HVE incidents nationally and may be subject to change.

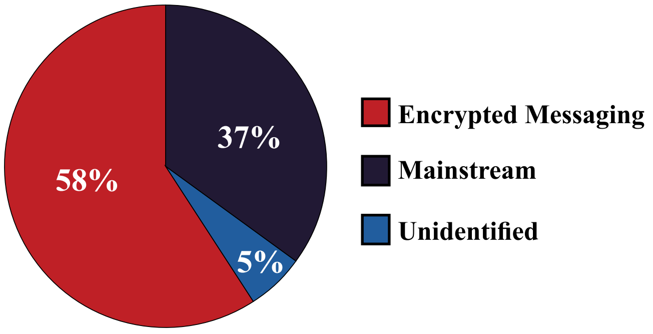
Threat Summary

An NJOHSP review of the data set identified notable statistics and trends among domestic extremists and HVEs and their use of social media, including platform type, pre-operational online activity, and ideological affiliation or group influence. In 2024, half of the domestic threat actors identified with white racially motivated extremist (WRME) ideology. This was followed by anti-government extremists, including sovereign citizen and militia extremists, which accounted for seven of the 20 individuals. They predominately operated on mainstream platforms to discuss their ideologies and post threats, which accounted for 45 percent of their online activity. In eight out of the 10 HVE incidents, individuals drew inspiration from ISIS. HVEs used encrypted messaging platforms in 58 percent of the identified cases. They primarily used social media platforms to discuss ideology and post threats (36 percent), followed by providing material support to FTOs (29 percent).

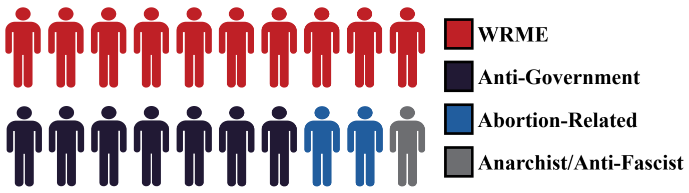
Domestic Extremist Platform Breakdown



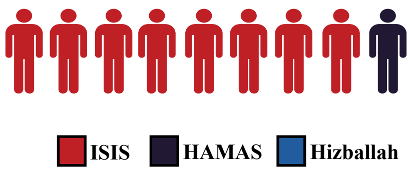
HVE Platform Breakdown



Domestic Extremist Ideology

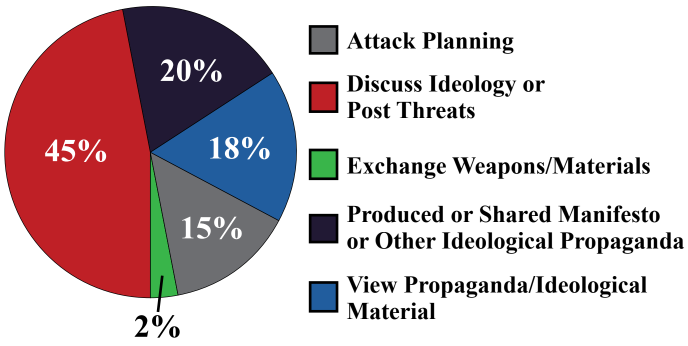


HVE Group Influence

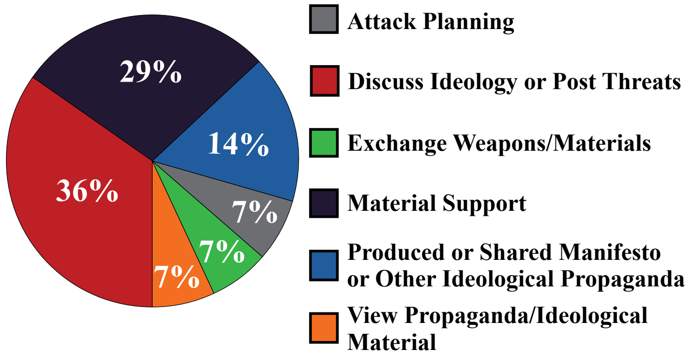


Domestic and Homegrown Violent Extremist Use of Social Media

Domestic Extremist Use of Social Media



HVE Use of Social Media



WRME Case Study

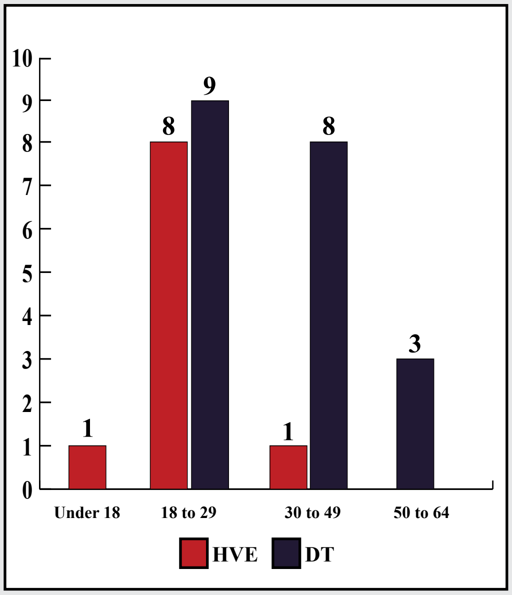
In June 2024, federal authorities arrested Hayden Espinosa of Texas for selling illegal firearms and weapons parts while incarcerated. Espinosa moderated a Telegram channel called "3D Amendment," where he sold the weapons and promoted WRME and accelerationist beliefs. On this channel, he sold items such as silencers, high-capacity magazines, handguns, and rapid-fire modification devices. Several members of the channel purchased firearms and parts from Espinosa and shared details of their purchases with other members. Espinosa also shared content on Telegram and YouTube promoting WRME ideology, neo-Nazi sentiments, and anti-government extremist beliefs.

HVE Case Study

In November 2024, federal authorities arrested Anas Said. In October 2023, the FBI received information regarding 11 Facebook accounts associated with Said, showing his continued support for ISIS and his desire to travel to join the group. Said allegedly used multiple encrypted messaging applications to consume news on ISIS-related channels and to create and disseminate propaganda glorifying ISIS's ongoing violence to at least 100 followers. Using social media, Said also discussed his desire to carry out violent attacks in the U.S. against military recruitment centers and the Jewish population.

Domestic Extremist and HVE Age Data

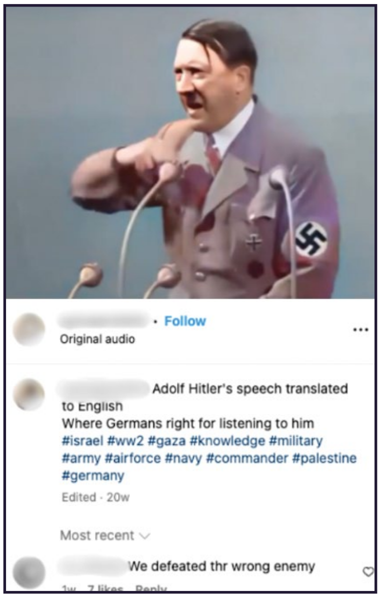
In 2024, while individuals between the ages of 18 and 29 primarily conducted domestic extremist and HVE incidents, a younger individual, Marvin Jalo, 17, also plotted to conduct an attack on behalf of ISIS. In October, authorities arrested Jalo in Phoenix, for using Telegram to discuss and procure the supplies necessary to construct an improvised explosive device. Jalo shared several videos of himself with the explosive materials and expressed his desire to use them against various targets, including the Phoenix Pride Festival and New York City. Similarly, in July, Andrew Takhistov, 18, of East Brunswick (Middlesex County) used Telegram to communicate on WRME-aligned channels to research body armor, disseminate manuals on how to construct various homemade guns, and praise mass shooters. Takhistov expressed his desire and plan to attack the power grid. He provided operational and tactical guidance to conduct the attack, including timing, constructing a Molotov cocktail, and avoiding detection.



Extremists Exploit GenAI to Recruit and Radicalize Online

Extremists exploit a range of generative artificial intelligence (GenAI) functionalities to expand recruitment and radicalization efforts online by engaging in mass production of propaganda, creating deepfakes, and allowing real-time interaction. GenAI presents opportunities for extremists to push targeted messaging to specific individuals online and reach new audiences in a quicker and more efficient manner than passively sharing content to broad audiences.

In September 2024, a neo-Nazi accelerationist group discussed viral videos containing English language AI-generated audio of Adolf Hitler on Telegram and noted that fellow neo-Nazis "should be making this content and spreading it." The group also shared that the content is being disseminated to large audiences at "lightning speed" compared to in-person propaganda distribution that may only reach smaller audiences. Similarly, ISIS-affiliated Telegram bots focus on sharing content, moderating conversations, and granting group membership. Research on the ISIS bots identified that the average bot posted 176 messages a day, including text, images, PDF documents, video clips, and audio files.



[redacted] · Follow
Original audio

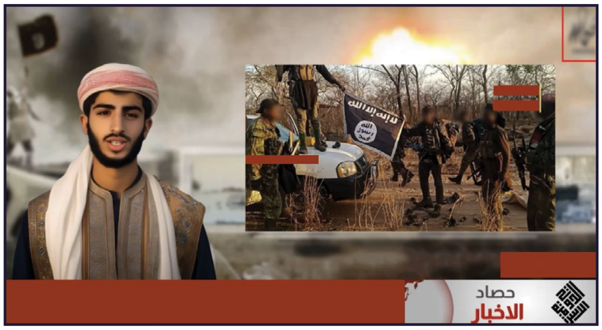
[redacted] Adolf Hitler's speech translated to English
Where Germans right for listening to him
#israel #ww2 #gaza #knowledge #military #army #airforce #navy #commander #palestine #germany
Edited · 20w

Most recent

[redacted] We defeated thr wrong enemy
1w 7 likes Reply

Translated Adolf Hitler content posted to Instagram.

In March 2024, ISIS supporters created an AI-generated media program called the *News Harvest*, which impersonates a recognizable mainstream media outlet, to disseminate propaganda videos. The program produces routine broadcasts featuring AI-generated news anchors discussing global ISIS operations. Extremists online are also using AI tools to develop and circulate English-language audio and video propaganda to rebrand Hitler as a "misunderstood" figure. These videos feature 20 to 30 second snippets of Hitler's speeches promoting white racially motivated extremist sentiments, such as antisemitic, anti-Muslim, and anti-immigrant messages. In 2024, these videos garnered over 50 million views across X, YouTube, TikTok, and Instagram.



Screenshot from AI-generated ISIS news video.

In February 2024, Gab released AI chatbots that allow users to interact with prominent historical figures, including Hitler and Osama bin Laden. These characters provide responses that are antisemitic, deny the Holocaust, and justify terrorist attacks. In January 2024, a researcher identified that an existing AI-powered website that allows users to create chatbots, produced bots designed to mimic extremist groups. One user-generated chatbot claiming to be a senior ISIS leader expressed its dedication to the terrorist organization and attempted to recruit the researcher. Similarly, 4chan users have used the same chatbot website to simulate different extremist groups, including one individual who represents an anti-fascist (Antifa) extremist and stereotypes of a "young liberal" who is part of the LGBTQ+ community.

Generative artificial intelligence (GenAI) is a form of AI that produces new content such as text, images, or videos by analyzing and learning from existing data patterns. This technology is easily accessible and user-friendly, even for individuals with limited technical skills, which increases the risk of potential misuse.

Counterintelligence

Threats From Foreign Actors

Nation-state actors and individuals working at the behest of foreign governments leverage strategies such as cyber intrusions and attacks, espionage, and theft to actively target critical infrastructure and evade laws to gain economic and military advantage over the U.S. Foreign adversaries such as China, Iran, and Russia have demonstrated the capability and intent to conduct malicious cyber operations against U.S. critical infrastructure, including energy, financial, healthcare, and telecommunications systems posing significant intelligence threats to the U.S.

Over the last few years, a diverse range of nation-state actors have targeted New Jersey through physical, cyber, and technical techniques that negatively impact private- and public-sector entities. Nation-state actors use trusted insiders such as employees and researchers, substantial financial investment, and other means to gain access to a company's valuable data. This can include theft of proprietary data, critical technology, and research; compromise of networks and supply chains; loss of competitive advantage or organizational reputation; and unforeseen legal liabilities.

Acknowledging foreign threats reinforces the need for robust counterintelligence measures, a proactive approach to cybersecurity, and continuous efforts to enhance national security and protect sensitive information in an ever-evolving global landscape.

In the global arena, nations recognize the importance of gathering intelligence on the U.S., a global superpower with significant political, military, technological, and economic influence. Various countries, both allies and adversaries, employ their intelligence agencies to collect information that can provide strategic advantages, shape policies, and protect their own interests. These intelligence operations range from traditional espionage activities, such as human intelligence gathering and signals intelligence, to more sophisticated cyber operations targeting government agencies, critical infrastructure, and corporate entities.

In November 2024, dual U.S.-Russian national and New Jersey resident Vadim Yermolenko, pleaded guilty to conspiracy to violate the Export Control Reform Act, conspiracy to commit bank fraud, and conspiracy to defraud the U.S. for his role in a transnational procurement and money laundering network that sought to acquire sensitive dual-use electronics for Russian military and intelligence services. Yermolenko, under the direction of Russian intelligence services, procured advanced electronics and sophisticated testing equipment for Russia's military industrial complex and research and development sector, according to court documents.

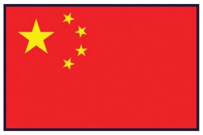
"China's hackers are positioning on American infrastructure in preparation to wreak havoc and cause real-world harm to American citizens and communities, if or when China decides the time has come to strike."

FBI Director Christopher Wray,
January 2024

In October 2024, federal authorities announced that a Chinese-backed hacking group, Salt Typhoon, gained access to and monitored at least nine telecom companies in the U.S., with dozens of other countries also affected, for as long as at least two years. The U.S. National Security Council said that "there is a risk of ongoing compromises to communications until U.S. companies address the cybersecurity gaps. The Chinese are likely to maintain their access." The attack provided the hackers access to multiple types of information, including call records, access to some specific phone calls, and systems where law enforcement and intelligence agencies, with a court order, can access phone calls and other data.

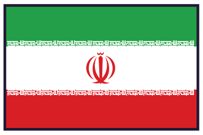
In February 2024, the FBI warned Congress that Chinese-government backed hackers "burrowed" into the United States' cyber infrastructure to cause damage, targeting water treatment plants, the electrical grid, transportation systems, and other critical infrastructure. In 2023 and 2024, six U.S. water facilities experienced significant cyber incidents, several of which nation-state cyber threat actors allegedly perpetrated.

Threats From Foreign Actors



People's Republic of China

As a major global power and economic competitor, China employs sophisticated intelligence operations aimed at acquiring sensitive U.S. technology, proprietary information, and national security secrets. The Chinese government utilizes a range of tactics, including cyber espionage, human intelligence efforts, and economic espionage, to systematically target U.S. government agencies, defense contractors, research institutions, and corporations. China's persistent and well-resourced approach poses a grave risk to U.S. national security, economic interests, and technological leadership. The threat extends beyond traditional espionage to encompass influence campaigns, supply chain vulnerabilities, and efforts to exploit academic and research partnerships.



Islamic Republic of Iran

Iran's intelligence agencies, particularly the Ministry of Intelligence and Security (MOIS) and the Islamic Revolutionary Guard Corps-Quds Force (IRGC-QF), pose a significant threat to U.S. interests. These agencies are responsible for conducting espionage, sabotage, and terrorist operations against U.S. targets globally. They have been linked to cyberattacks on U.S. critical infrastructure, theft of sensitive technology and intellectual property, and attempts to recruit U.S. persons to spy on behalf of Iran. Iran's intelligence agencies have been involved in plots to assassinate U.S. officials and disrupt U.S. military operations in the Middle East. The U.S. government has designated both MOIS and IRGC-QF as foreign terrorist organizations, highlighting the serious nature of the threat they pose to U.S. national security.

Russian Federation

As a formidable adversary with a long history of intelligence operations, Russia utilizes a range of tactics to undermine U.S. national security interests. These methods include cyber espionage, disinformation campaigns, influence operations, and targeted attacks on critical infrastructure. Russia's intelligence agencies, particularly the Foreign Intelligence Service (SVR) and the Main Intelligence Directorate (GRU), demonstrate sophistication and adaptability in their operations. Often employing highly trained, career intelligence officers, their activities aim to exploit vulnerabilities in U.S. government agencies, political systems, technology sectors, and public opinion to advance Russia's strategic goals.

Countering these threats demands a comprehensive and multi-faceted approach, combining robust cybersecurity measures, rigorous vetting processes, strengthened intelligence cooperation, and stronger laws and strategic policy initiatives to safeguard America's critical assets and maintain its competitive edge in an increasingly complex global landscape.

NJ Office of Homeland Security and Preparedness

Transnational Criminal Organizations

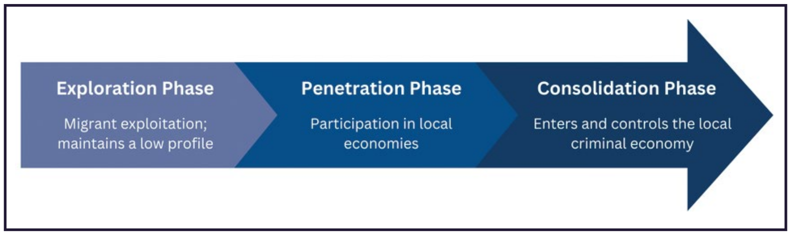
Transnational Criminal Organization Activity in New Jersey

Key Findings

The New Jersey Regional Operations and Intelligence Center (NJ ROIC) continues to assess the impact of transnational criminal organizations (TCOs) engaging in criminal activity throughout New Jersey into 2025. The NJ ROIC has analyzed publicly available information indicating specific public safety threats from TCOs, including Tren de Aragua (TdA) and other South American Theft Groups (SATGs) that identify New Jersey as an attractive location for illicit activities due to the proximity between two major urban centers. The NJ ROIC expects recruitment operations to increase as suspected TdA and SATG members may continue to expand their presence by building an expansive association network in New Jersey to conduct criminal activities such as targeted high-end robberies and organized retail theft.

Tren de Aragua Criminal Syndicate (TdA)

TdA emerged at the Tocorón prison in the Venezuelan state of Aragua. TdA differs from common U.S.-based street gangs due to its political influence generated from the Venezuelan government's unofficial policy of handing control of prisons over to its local criminal leaders. Originally, TdA members extorted businesses during the Venezuelan economic crisis, however, they have since expanded their criminal activities into narcotics and human trafficking.


Exploration Phase
Migrant exploitation; maintains a low profile
Penetration Phase
Participation in local economies
Consolidation Phase
Enters and controls the local criminal economy

Tren de Aragua's expansion phases.

TdA is believed to have arrived in the U.S. between 2021 and 2022 and has grown their presence here by exploiting border vulnerabilities and penetrating local criminal enterprises. While similarly engaging in organized theft such as SATGs, TdA activities also include extortion, kidnapping, human trafficking, human smuggling, drug and weapons trafficking, and homicide. The U.S. Department of the Treasury designated TdA as a transnational criminal organization in July 2024.

South American Theft Groups (SATGs)

SATGs are comprised largely of South American foreign nationals, mainly from Chile and Colombia, who enter the U.S. with the sole purpose of committing highly organized luxury home and retail burglaries. Chilean SATG members are suspected of exploiting the U.S. Department of Homeland Security's (DHS) Visa Waiver Program, which allows designated nationals to visit the U.S. for 90 days without a background check, to conceal their criminal backgrounds. Members of SATGs are involved in various criminal activities including thefts of designer merchandise, cash, watches, and jewelry. The NJ ROIC has determined that SATGs have taken advantage of New Jersey's densely populated regions by targeting a wide range of retails stores statewide to expand their revenue streams. Once these acts are completed, they dispatch their earnings back home.

More sophisticated SATG members have been reported to conduct preoperational surveillance of a desired target. In coordination with DHS partners, the NJ ROIC has identified some of these preoperational planning efforts which include scouting a desired storefront and exterior parking areas; spray painting security camera lenses; using signal jammers and aerial drones; and using GPS to track potential victims' devices.

Current Threat Environment

- **December 10, 2024:** The National Football League (NFL) issued a security alert after SATGs targeted multiple NFL and National Basketball Association players' homes.
- **December 9, 2024:** Enforcement and Removal Operations Newark arrested twelve noncitizens from Chile, Colombia, and Peru connected to SATGs on immigration charges.
- **June 13, 2024:** A suspect linked to a SATG used a Wi-Fi jammer in an unsuccessful burglary attempt in Florham Park (Morris County).
- **May 20, 2024:** Authorities arrested four men associated with SATGs in connection with multiple home burglaries in Bernards Township (Somerset County).

Implications for New Jersey

- TdA and the SATGs have expanded their presence around New Jersey and the NJ ROIC expects them to continue to conduct illicit activities in the region.
- TCOs are expected to continue to exploit the security environment at the border to conduct illicit activities in the U.S.
- TdA and SATG members are expected to continue to carry out retail thefts and high-end robberies in 2025.

NJ Office of Homeland Security and Preparedness

Cybersecurity Threats

Cybersecurity Threats

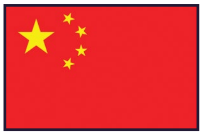
The New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) assesses with high confidence that in 2025 and beyond, cyberattacks against New Jersey public and private institutions, critical infrastructure assets, and residents will increase in volume and impact. These attacks will be operationally debilitating and costly and will adversely impact public health, the welfare and safety of our residents, the economy and public interests of the State, and national security.

The NJCCIC is a division within the New Jersey Office of Homeland Security and Preparedness. It acts as the State's central civilian interface for coordinating cybersecurity information sharing, performing cybersecurity threat analysis, and promoting shared and real-time situational awareness between and among the public and private sectors. It is also charged with the development and execution of the enterprise cybersecurity strategy for the New Jersey State Executive Branch. This cybersecurity threat assessment is based on the analysis of data collected from the NJCCIC's cybersecurity tools, technologies and services, incident and data breach reports made to the NJCCIC, threat intelligence shared with the NJCCIC by its public- and private-sector partners, and open and commercial sources of cyber threat information and intelligence.

The NJCCIC 2025 threat assessment is informed by key trends, significant incidents, threat actor capabilities, systemic risks, and technological advancements over the past several years and provides actionable insights for enhancing New Jersey's cybersecurity posture.

Cyber Threat Landscape

Every day, New Jersey's public and private institutions and its residents face a relentless wave of cyberattacks from a wide range of threat actors with varying capabilities and motives. Nation-state adversaries such as China, Russia, Iran, and North Korea continue to target U.S. companies and infrastructure to advance their respective military, political, and economic agendas. Some examples of current nation-state threats include:



China's Cyber-Physical Threats to U.S. Critical Infrastructure (Volt Typhoon and Salt Typhoon)

China's President Xi Jinping has ordered China's military to prepare for a potential invasion of Taiwan by 2027. In addition to the military buildup by China's People's Liberation Army (PLA) at home, the PLA is also carrying out at least two significant cyber operations, coined Volt Typhoon and Salt Typhoon, targeting critical infrastructure in the U.S. As part of Volt Typhoon operations, China has been prepositioning (gaining undetected and unauthorized access) to U.S. critical infrastructure networks and systems, including but not limited to those in the telecommunications, transportation, energy, water, and healthcare sectors so that it can obstruct the U.S.' ability from coming to the aid of Taiwan. In the Salt Typhoon operations, China has gained access to at least nine major U.S. telecommunications providers, including AT&T and Verizon, for espionage purposes - listening in on the calls of high-value targets and collecting the metadata (call detail records) of these carriers' customers.

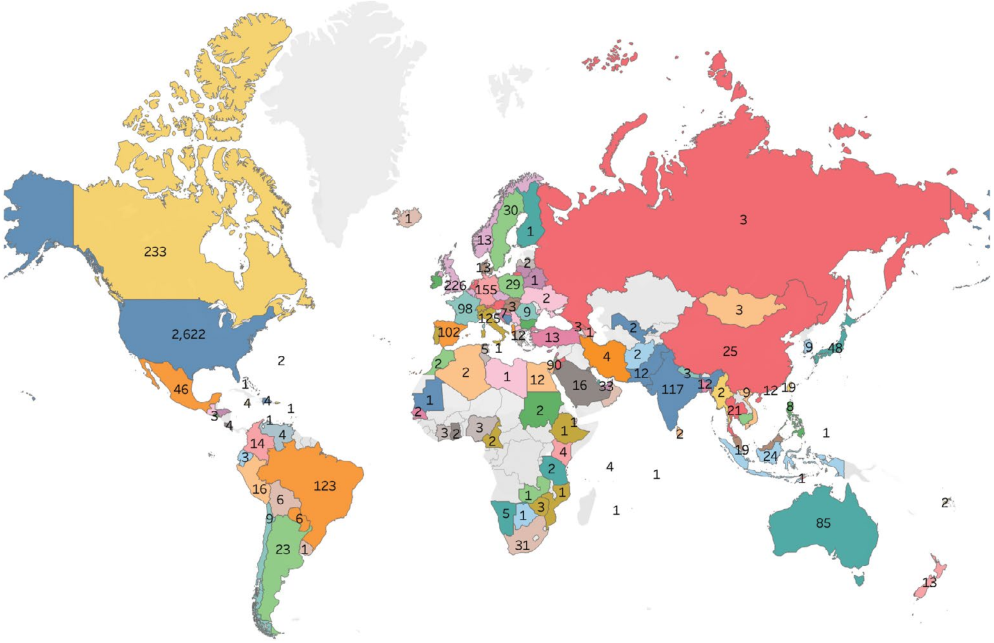
By prepositioning themselves on U.S. critical infrastructure networks and systems, China can disable power grids, disrupt transportation systems, compromise water treatment facilities, and create widespread chaos in New Jersey and across the U.S. According to former FBI Director Christopher Wray and former U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency Director Jen Easterly, China poses the greatest long-term threat to U.S. national security. Salt and Volt Typhoon are just two examples of their capabilities and threat.

Russia's Midnight Blizzard Espionage Operation

Midnight Blizzard, also known as NOBELIUM, APT29, and Cozy Bear, is a sophisticated Russian state-sponsored cyber espionage group tied to Russia's Foreign Intelligence Service (SVR). Its operations primarily focus on intelligence collection, targeting government agencies, think tanks, and technology companies in Western countries. The group is known for its advanced persistent threat (APT) tactics, including supply chain compromises, sophisticated social engineering, and the ability to maintain long-term undetected access to compromised networks.

One of its most notable operations involved compromising Microsoft's corporate email system in late 2023 into early 2024, where it targeted senior Microsoft executives and accessed email accounts containing information about Midnight Blizzard itself. While inside Microsoft's network, the threat actors also gained access to the company's customers' emails, including that of federal and state government organizations. This incident demonstrated its sophisticated capabilities in password spraying attacks and its focus on gathering intelligence about how it was being investigated and tracked. The group has also been linked to other significant compromises, including the SolarWinds supply chain attack in 2020, which affected thousands of organizations globally and demonstrated its ability to conduct complex, large-scale cyber espionage operations.

While nation-state cyberattacks are focused on the respective country's strategic interests, financially motivated cybercriminal organizations—including LockBit, Clop, RansomHub, ALPHV/Blackcat, and others—have continued to carry out lucrative yet debilitating ransomware attacks against a broad spectrum of targets, including critical infrastructure, state and local governments, law enforcement agencies, businesses of all sizes, and educational institutions. In 2024 alone, the NJCCIC tracked over 5,600 ransomware attacks worldwide that were publicly disclosed on threat actors' leak websites and other platforms. Of those, more than 2,600 victims were in the U.S., including 105 public and private organizations in New Jersey. In the first half of 2024, the average ransom demand increased to $1.9 million, while the average ransom payment amounted to approximately $479,000. It should be noted that fewer victims are paying ransoms and opt to recover systems and services from backups instead.



Ransomware victims by country in 2024.

Notable 2024 ransomware incidents included:

Change Healthcare: In February 2024, Change Healthcare, a subsidiary of UnitedHealth Group and a major healthcare claims processor in the U.S., suffered a significant ransomware attack that encrypted critical data and disrupted operations. The ALPHV/BlackCat ransomware group accessed the Change Healthcare network using compromised credentials for a Citrix remote access service that lacked multifactor authentication. In addition to encrypting systems, ALPHV/BlackCat exfiltrated approximately six terabytes of sensitive personally identifiable information and protected health information, including health insurance member IDs, patient diagnoses, treatment details, and Social Security numbers of over 190 million individuals, making it the largest healthcare data breach in U.S. history. In response, UnitedHealth Group paid a ransom of $22 million in an attempt to prevent the dissemination of the stolen data. As of January 2025, Change Healthcare is still recovering from the attack and has thus far incurred approximately $2.9 billion in total costs, including those associated with direct response efforts, business disruptions, and advanced payments to affected healthcare providers.

New Jersey City University: In June 2024, New Jersey City University (NJCU) fell victim to a ransomware attack that exposed sensitive personal and financial information of approximately 297,000 past and current students and staff. The data included Social Security numbers, driver's license numbers, financial account details, and credit card information. The Rhysida ransomware group carried out the cyberattack and demanded a ransom payment of approximately $700,000; NJCU declined to pay. The university shut down some systems and services for several weeks while it recovered from the attack.

Veolia: In January 2024, Veolia North America, which manages 416 water and wastewater systems serving 27 million U.S. customers, including approximately 260,000 customers in New Jersey, suffered a ransomware attack targeting its municipal water division. The attack, carried out by the Black Basta ransomware group, affected various software applications and internal back-end systems, leading the company to temporarily take these systems offline to contain the threat and initiate restoration efforts. These measures resulted in delays for customers attempting to use online bill payment services. No water or wastewater treatment operations were impacted.

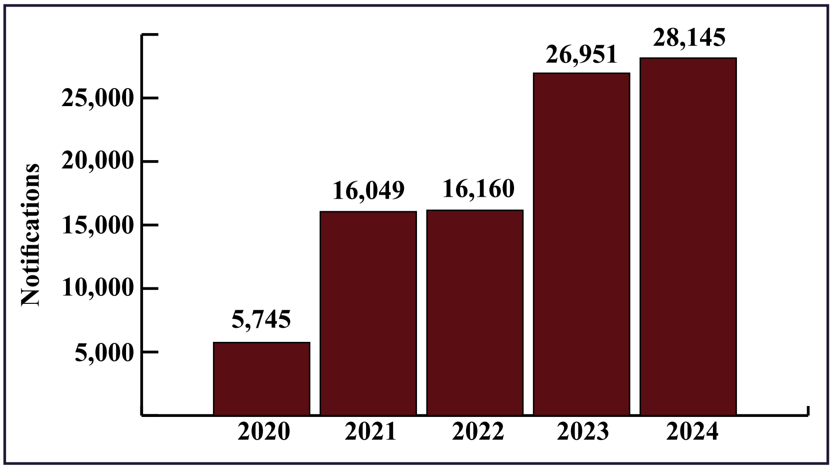
Port of Seattle: In August 2024, the Port of Seattle, which operates Seattle-Tacoma International Airport fell victim to a ransomware attack orchestrated by the Rhysida ransomware group. The attack led to widespread service disruptions, affecting baggage handling systems, check-in kiosks, ticketing services, passenger information displays, airport Wi-Fi, the Port of Seattle website, the flySEA mobile app, and reserved parking services. The attack created significant operational challenges, particularly for smaller airlines that rely on shared technology systems. As a result, airline staff had to revert to manual processes, handwriting boarding passes and bag tags to keep flights moving. The Port of Seattle refused to pay the $6 million ransom demand, instead opting to recover services from backups. The full recovery of the Port's services took more than a month.

City of Hoboken: In late November 2024, the City of Hoboken (Hudson County) fell victim to a ransomware attack that disrupted municipal operations. The attack, attributed to the ThreeAM ransomware group—a faction possibly linked to the notorious Conti cybercrime organization—led to the temporary closure of City Hall and the suspension of online services. Essential functions such as the municipal court and street cleaning were also affected. As of December 2024, Hoboken officials continued working with cybersecurity specialists and the FBI to determine the incident's source, scope, and nature.

These and other notable ransomware attacks demonstrate that no sector is immune. Government, healthcare, water and wastewater, and other critical infrastructure sectors are prime targets for ransomware actors due to the urgent need to restore services. This urgency often pressures victims into making ransom payments to threat actors rather than enduring prolonged outages. Furthermore, the additional threat of releasing sensitive stolen data provides additional pressure for victims to pay ransom demands.

The Growing Threat of Stolen Login Credentials

Compromised credentials remain one of the most prevalent initial access vectors in cyber intrusions, frequently exploited by threat actors to bypass authentication mechanisms and gain unauthorized access to victim networks and systems. Credentials are often obtained through phishing campaigns, large-scale data breaches, or credential stuffing attacks, where previously leaked username-password pairs found on underground sites are systematically tested across multiple platforms. Threat actors use weak or compromised credentials in all manner of cyberattacks. Several high-profile cyberattacks highlight the danger of compromised credentials, including the 2021 Colonial Pipeline incident, the 2024 breaches of Change Healthcare, Snowflake, and PowerSchool, and the Cyber Army of Russia Reborn's (CARR) attacks on U.S. water systems in 2024.



NJCCIC compromised credentials notifications.

An increasingly common method of obtaining compromised credentials involves using stealer malware, which extracts login credentials, session tokens, and other sensitive authentication data directly from an infected endpoint. Estimates indicate anywhere from one million to more than 10 million computers are currently infected with stealer malware, such as RedLine Stealer, Raccoon Stealer, Lumma, Vidar, and others.

Stealer malware targets credential stores within web browsers, password managers, and system memory. Once executed on a compromised machine, these malware strains enumerate saved credentials, exfiltrating them to command-and-control (C2) servers operated by attackers. The stolen credentials are then leveraged for unauthorized access, privilege escalation, and lateral movement within enterprise environments. Since credential-based attacks require no malware deployment and rely on legitimate authentication workflows to facilitate persistence, they often evade traditional endpoint detection systems. Studies indicate that weak or stolen credentials account for over 80 percent of hacking-related breaches. To combat such attacks, the NJCCIC proactively searches for compromised credentials (email addresses/passwords) published to the dark web, paste sites, and other internet sites belonging to New Jersey public sector personnel and select critical infrastructure personnel. Published email addresses in scope are limited to work and school accounts.

Notifications by Sector (2024)	
Sector	**Count**
Education Sector	**26,128**
Water Sector	**768**
Healthcare Sector	**553**
State Government	**355**
Municipal Sector	**163**
County Government	**122**
Law Enforcement	**56**
Totals	**28.145**

NJCCIC compromised credentials notifications by sector in 2024.

In 2024, the NJCCIC made 28,147 notifications, up from 26,951 in 2023, to affected New Jersey organizations of their compromised employee and/or student login credentials and instructions for mitigating the risk of their potential misuse. Compromised login credentials are a favored method for threat actors to gain unauthorized network access, often without detection, by appearing as legitimate logins. Various reports estimate over 15 billion sets of compromised credentials are available on the internet. As such, this attack vector is expected to remain a top choice for threat actors targeting New Jersey public- and private-sector organizations, as well as the state's residents in 2025.

Threat Actor Group Alliances

In the past, the term "advanced persistent threat" was reserved primarily for well-resourced and highly capable nation-state threat actors such as governments, military units, or intelligence directorates. However, with the increasing technical capabilities of cybercrime syndicates, hacktivist groups, and freelance threat actors, the lines that separate them have become blurred. Just in the past two years, there is evidence that Russian ransomware actors and hacktivist groups, such as Conti and CARR, have been tasked by the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU) to conduct cyberattacks on Russia's behalf. In 2024, CARR and an associated Russian hacktivist group, Z-Pentest Alliance, targeted and compromised the industrial control systems and operational technologies of water and wastewater, energy, and manufacturing systems of critical infrastructure owners and operators throughout the U.S., including four municipal water systems in New Jersey. NoName-57(16), another prolific Russian hacktivist group, continues conducting large-scale distributed denial-of-service (DDoS) attacks against Western countries' public- and private-sector networks. These DDoS attacks have disrupted the operations of numerous federal, State, and local governments, healthcare providers, and critical infrastructure owners and operators worldwide.

The Iranian hacktivist group CyberAv3ngers is supported by and aligned with the Islamic Revolutionary Guard Corps. The People's Liberation Army of China's cyber component is an amalgamation of government, military, and corporate actors working together. Even within the cybercrime community, Western hacking groups, such as Scattered Spider, have formed alliances with Russian ransomware threat actors to conduct mutually beneficial operations. New partnerships between groups are announced daily in the hacktivist underworld on Telegram. The NJCCIC expects such alliances to continue to grow as there is further alignment of mutual goals and interests among the diverse threat actor groups, further blurring the lines between these groups and obfuscating attribution for their attacks.

Cyber-Enabled Fraud

As with ransomware attacks in which the motivation of the threat actors is financial, cyber-enabled fraud is a growing threat, with losses by U.S. victims exceeding over $10 billion annually. Cyber-enabled fraud scams have become increasingly sophisticated and prevalent, leveraging technology to deceive victims and steal money or sensitive information. The NJCCIC categorizes these scams under the umbrella term of social engineering, as they all involve the manipulation of individuals into divulging sensitive information, granting unauthorized access, or performing actions that compromise security. Instead of exploiting technical vulnerabilities, social engineering exploits human psychology, leveraging tactics such as deception, urgency, and trust-building to achieve fraudulent objectives. Social engineering plays a key role in many cyber-enabled fraud schemes, including business email compromise (BEC) attacks as well pig butchering and tech support scams, etc.

BEC: Unlike generic phishing campaigns, BEC scams are a highly targeted form of social engineering. To make messages appear more legitimate, attackers commonly spoof a familiar contact's source name or email address, use email domains that mimic a trusted source, or compromise a legitimate business account. The body of these messages often instructs the recipient to transfer funds or other sensitive information to the threat actor posing as a trusted associate. In 2023, Americans lost nearly $3 billion due to BEC scams, a nine percent increase over 2022, according to the FBI. The NJCCIC regularly receives reports from New Jersey organizations targeted by BEC phishing emails that attempt to steal funds or extract sensitive information.

Pig Butchering Scams: Pig butchering is a sophisticated financial scam in which fraudsters cultivate trust with their victims over weeks or even months before luring them into fraudulent investments. The scheme often begins with friendly or romantic interactions on social media or messaging apps, where scammers present themselves as legitimate and successful individuals, frequently boasting about their supposed wealth from cryptocurrency or forex trading. Once they have built rapport, they introduce what appear to be legitimate investment opportunities, directing victims to professional-looking but entirely fake trading platforms. The term "pig butchering" comes from how scammers "fatten up" their targets by allowing small initial gains to build confidence before ultimately stealing large sums. Since these transactions often involve cryptocurrency, recovering the stolen funds is extremely difficult. These scams are increasingly sophisticated, often run by organized crime syndicates operating across multiple countries, particularly in Southeast Asia. Many of the individuals carrying out the scams are themselves victims of human trafficking, initially deceived with promises of legitimate jobs in customer service but later forced by criminal organizations to perpetrate fraud.

In 2023, a pig butchering scam led to the collapse of Kansas-based Heartland Tri-State Bank when its CEO lost $47 million to unidentified fraudsters, forcing a Federal Deposit Insurance Corporation takeover. Victims of "investment frauds," which overlap with pig butchering, reported losses of $4.6 billion to the FBI in 2023, up from $3.3 billion in 2022. The NJCCIC has documented multiple cases of New Jersey residents falling victim to such schemes. The growing popularity of cryptocurrency and the belief that it is a lucrative investment vehicle virtually ensures such scams and the resultant losses by its victims will continue to increase in 2025 and beyond.

Tech Support Scams: In the past several years, tech support scams have become increasingly prevalent, with fraudsters impersonating employees from reputable companies, such as Microsoft and Apple, to deceive unsuspecting individuals. These scammers often initiate contact through unsolicited phone calls, emails, or pop-up messages, falsely claiming that a user's computer is infected with malware or experiencing technical issues. They create a sense of urgency, pressuring victims into granting remote access to their devices or purchasing unnecessary software and services. Once access is obtained, scammers may install malware, steal personal information, or demand payment for fictitious support services. In 2023 alone, the FBI's Internet Crime Complaint Center reported that tech support fraud cost victims nearly $1 billion. As with other lucrative money-making fraud efforts, tech support scams are expected to grow in 2025.

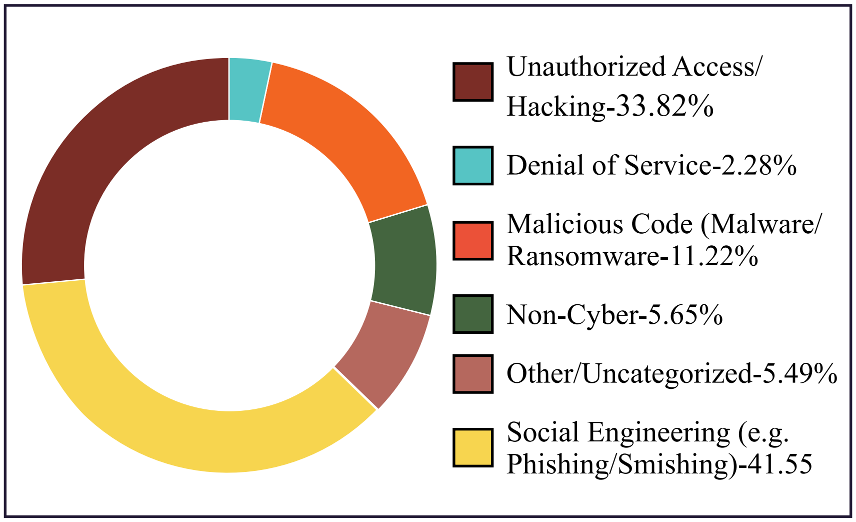
In addition to the above examples, there are many more types of cyber-enabled fraud schemes, including employment scams, romance scams, imposter scams, elder fraud, etc. Often, the themes of the scams are blended depending on the targets. Over the past four years, social engineering schemes were the cyber incident type most reported to the NJCCIC, at 42.21 percent (1,075 of the 2,547 reports).

Cyber-enabled fraud scams have resulted in significant financial losses. In the U.S., the Federal Trade Commission reported that Americans lost over $10 billion to scammers in 2023. Given the rising trend in cyber-enabled fraud, the total losses for 2024 are anticipated to surpass that figure. Generative AI (GenAI) tools aid scammers in generating highly convincing personalized phishing emails, fake identities, deepfakes, and other deceptive content, making it much easier to trick victims into sharing sensitive information or transferring money. These communications are more difficult to detect than traditional scams as they will appear legitimate, allowing scammers to scale their fraudulent activities with greater sophistication and reach.

Incident Reporting

In 2024, the NJCCIC received 514 cybersecurity incident reports through its incident reporting portal. Of these, 149 were reported by public agencies in accordance with P.L. 2023, c.019. When the law was enacted in 2023, the NJCCIC received 141 cybersecurity incident reports from public agencies, and in 2022, prior to the reporting law, the NJCCIC received 96 reports from public agencies.

However, not all cyberattacks are reported to the NJCCIC. In addition to the reports made to the NJCCIC via its reporting portal, the NJCCIC also proactively notifies organizations whose information technology (IT) infrastructure has been compromised or whose networks contain vulnerabilities that threat actors could exploit. The NJCCIC does this due to indicators of compromise it detects, information provided by trusted third parties, and other open and commercial intelligence sources. In 2024, the NJCCIC notified 227 public- and private-sector organizations that their IT infrastructure had been compromised.



Incident types reported to the NJCCIC from 2020 to 2024.

The NJCCIC reasonably believes that the number of cybersecurity incidents suffered by New Jersey organizations and individuals is much greater than those reported and those for which the NJCCIC notified the impacted entities.

The Value of Incident Reporting: Timely and thorough reporting of cybersecurity incidents to the NJCCIC is essential for the following reasons:

1. Enhanced Response and Recovery: When incidents are reported to the NJCCIC, affected organizations gain access to specialized expertise, including threat analysis, remediation guidance, and coordination with law enforcement and other resources that can provide response and recovery assistance. In addition, the reporting entity can receive assistance in implementing controls to bolster its cybersecurity posture and help ensure it does not experience a reoccurrence.

2. Improved Threat Intelligence: Each report helps the NJCCIC build a clearer picture of the threat landscape, allowing for the identification of emerging trends. For example, reports of phishing campaigns and ransomware attacks have informed advisories and alerts the NJCCIC has published that helped other organizations prevent similar incidents.

3. Preventing Cascading Failures: Cyberattacks often have ripple effects. Reporting incidents allows the NJCCIC to warn potentially impacted sectors and prevent broader disruptions.
4. Strengthened Public- and Private-Sector Collaboration: Incident reporting fosters collaboration between public agencies, private businesses, and federal partners, creating a unified defense against cyber threats. This collaboration is vital in addressing systemic risks.

Geopolitics and its Impact on the Threat Landscape

In 2025, geopolitical cyber threats will continue to evolve as nation-state actors intensify their cyber operations, targeting governments, critical infrastructure, and private enterprises. The NJCCIC assesses that state-sponsored cyber activity will remain a top threat, with adversaries using espionage, cyber sabotage, and influence operations to advance their strategic interests. Russia, China, Iran, and North Korea remain the most active cyber adversaries, each leveraging increasingly sophisticated tactics and techniques to undermine U.S. security, disrupt critical industries, and exploit emerging technologies.

Key factors that may shape the cyber threat landscape in 2025 include the transition from a Biden to a Trump administration, the recent ceasefire between Israel and Hamas, the ongoing Russia-Ukraine war, and China's continued push for the reunification of Taiwan.

Artificial Intelligence Threats

Over the past several years, the rapid evolution and widespread adoption of GenAI technologies have brought unparalleled opportunities and significant cybersecurity challenges. AI-driven advancements are reshaping industries, enhancing automation, and improving decision-making, but they are also empowering cybercriminals with new attack capabilities.

The NJCCIC assesses with high confidence that threat actors will increasingly exploit GenAI to create highly convincing and personalized phishing campaigns at scale. By leveraging artificial intelligence's (AI) ability to craft human-like emails, texts, and voice messages, attackers will bypass traditional phishing detection tools and increase the success rate of their scams. Meanwhile, the rise of deepfake technology has introduced a new era of deception, where fabricated audio and video content is being weaponized for fraud, disinformation campaigns, and political manipulation. Adversaries are already deploying deepfakes to impersonate executives in financial scams, spread misinformation on social media, and influence political processes by sowing distrust and undermining election integrity.

Beyond deception, AI is revolutionizing threat actor cyber tactics. Microsoft, OpenAI, and Google have reported instances of threat actors from Russia, China, Iran, and North Korea using their AI platforms for research, target reconnaissance and vulnerability identification, task automation, content translation, and malware development. As AI models become more sophisticated, they will amplify the scale and efficiency of cyberattacks, posing greater risks to organizations, governments, and individuals.

While AI presents transformative benefits, its unchecked proliferation poses significant security risks. Many AI vulnerabilities remain unknown, requiring proactive measures to identify, mitigate, and regulate potential threats. Governments and industries must implement robust AI governance models, ethical frameworks, and risk management strategies to safeguard against AI-enabled cyberattacks. Addressing these challenges requires global collaboration, continuous threat intelligence monitoring, and adaptive cybersecurity defenses to ensure that AI serves as a tool for progress rather than a weapon for exploitation.

Systemic Cyber Risk

Systemic cyber risk refers to the potential for a cyber incident, whether caused by intentional, accidental, or natural events, to trigger widespread disruption across multiple organizations, sectors, or economies. In today's hyper-connected world, systemic cyber is exacerbated by several compounding factors, including but not limited to insecure and misconfigured devices and software platforms, fragile supply chains, lack of visibility into third-party networks, technological debt, inequities in cyber defense capabilities, and an ever-increasing dependence of technology for all facets of commerce, government, education, and society at large. Systemic cyber risk poses a significant threat to public- and private-sector entities and individuals, potentially disrupting critical infrastructure, economic stability, and public safety. Three notable cyber incidents, one accidental and two malicious, that underscore the consequences of systemic cyber risk include:

CrowdStrike Faulty Update (2024): In July 2024, a faulty update from the cybersecurity firm CrowdStrike resulted in a global IT outage in which approximately 8.5 million Windows devices crashed. This incident disrupted critical sectors, including airlines, banks, and healthcare services, causing flight cancellations, financial losses, and operational halts across multiple industries.

Viasat Hack (2022): At the outset of the Russia-Ukraine war in February 2024, Russia carried out a cyberattack against the U.S. communications company Viasat's KA-SAT broadband satellite service with the intent of reducing the capabilities of Ukraine's military command and control networks. However, the cyberattack had far-reaching impacts beyond Ukraine's military systems as it also impacted civilian networks in Ukraine and beyond. Throughout Europe and the Middle East, approximately 50,000 customers lost internet service due to the attack. Russia's attack on Viasat also impacted the German energy company Enercon, which lost remote monitoring access to over 5,800 wind turbines.

NotPetya (2017): In June 2017, the GRU inserted malware into an accounting software update, which resulted in the most damaging cyberattack in history. While the malware was intended to target and weaken businesses operating in Ukraine, its destructive nature spread worldwide, impacting Merck, Maersk, and the Port Newark Container Terminal in New Jersey. This cyberattack is known as NotPetya and resulted in more than $10 billion in damages worldwide, including over $1.4 billion in New Jersey alone.

These incidents, and many more (e.g., Change Healthcare, PowerSchool, Midnight Blizzard), demonstrate how a single cyber incident can have far-reaching consequences.

Conclusion

New Jersey faces an escalating wave of sophisticated cyberattacks that threaten the state's essential operations and security. The NJCCIC assessment for 2025, based on current attack patterns, threat actor capabilities, geopolitical tensions, and systemic vulnerabilities, indicates that both public and private sectors will endure increasingly costly and disruptive attacks. These cyber threats pose direct risks to public health and safety, critical infrastructure, as well as the economic and national security interests within New Jersey. In such a complex and expanding threat environment, effectively managing cyber risk requires a proactive and collaborative approach. Public sector organizations at the federal, state, and local levels, as well as the private sector and large and small businesses, must collaborate by sharing threat intelligence, implementing robust cybersecurity standards, and fostering a culture of vigilance.

Resources

New Jersey Statewide Threat Assessment Team (NJ STAT)

NJ STAT is a joint initiative between federal, State, county, and local agencies that helps to effectively identify, assess, and intervene as needed to prevent escalation by individuals who are at risk of conducting a targeted act of violence.

The NJ STAT Steering Committee includes members from:

- ☑ New Jersey Office of Homeland Security and Preparedness (NJOHSP)
- ☑ New Jersey Department of Education (NJ DOE)
- ☑ New Jersey Department of Human Services (NJ DHS)
- ☑ New Jersey Office of the Attorney General (NJ OAG)
- ☑ New Jersey State Police (NJSP)
- ☑ Federal Bureau of Investigation (FBI)
- ☑ United States Secret Service (USSS)

NJ STAT provides alternative avenues for individuals who exhibit concerning behaviors and may be on the pathway to violence. NJ STAT utilizes the New Jersey Suspicious Activity Reporting System (NJSARS) as the primary method of identifying individuals of concern. As mandated by the New Jersey Attorney General Directive 2016-7, NJSARS will continue to serve as the main hub for collecting data concerning suspicious or criminal activities potentially linked to terrorism and threats of violence against both hard and soft targets. NJSARS is one of the primary referral mechanisms for behavioral threat-related cases supported by NJ STAT. From 2019 to 2024, a review of the NJSARS revealed a sharp increase in the number of school and community-based threats which required a multidisciplinary response and management process. All NJ STAT reports are reviewed and assessed for mobilization to violence indicators. Individuals identified with behavioral threat markers and the potential to become targeted violence actors are either referred to NJ STAT for comprehensive threat assessment/threat management or referred to county threat assessment teams or the NJ DOE Behavioral Threat Assessment and Management Teams (BTAMs) for further assessment.

Update for 2024/2025: As part of the New Jersey Statewide Targeted Violence Prevention Strategy, NJ STAT is working with all 21 counties on the creation of county threat assessment teams (CTATs). The goal is to establish county teams with the ability to conduct threat assessments and formulate effective mitigation strategies for individuals on a pathway to violence. Integral to the long-term success of the CTATs is the incorporation of partnerships across all levels of county government, including non-traditional partners such as mental health professionals, to establish effective teams. The addition of CTATs in a coordinated statewide effort will greatly enhance the State's ability to identify and mitigate threats of targeted violence.

NJ STAT Success Stories:

Through ongoing outreach efforts and collaboration with relevant stakeholders, NJ STAT has leveraged available resources and partnerships to successfully mitigate threats posed by both juveniles and adults on the path to committing targeted acts of violence. Two recent examples are:

- In the summer of 2024, NJ STAT was alerted to an incident of a juvenile who reportedly sent a letter to Brenton Tarrant, the perpetrator of the mass shooting in New Zealand in 2019. NJ STAT convened with law enforcement and school personnel, and learned additional information of troubling patterns of behavior, prompting the case to be escalated for further investigation. NJ STAT ensured that all partners were notified, to enable intervention and long-term support.
- In late 2023, NJ STAT received a report of a juvenile dressed up as Eric Harris, one of the Columbine school shooters, for Halloween. The juvenile also posted online videos emulating the school shooter, and demonstrated vast knowledge of the attack. In 2024, through collaboration with partners, NJ STAT was instrumental in facilitating communication amongst the school, mental health, and law enforcement partners, while monitoring the juvenile's needs and ensuring public safety remained a priority.

Interfaith Advisory Council

Created in 2012, the New Jersey Interfaith Advisory Council (IAC) is a network designed to facilitate information sharing and dissemination between law enforcement and faith-based organizations and communities around New Jersey.

The IAC, led by the New Jersey Office of Homeland Security and Preparedness (NJOHSP), allows NJOHSP and State leadership to maintain an ongoing dialogue with all faith-based groups, across all 21 counties in New Jersey, wishing to participate. The Director of NJOHSP chairs the council.

Quick Facts

- The IAC has a current membership base of approximately 4,000, all of whom have been vetted by NJOHSP program coordinators.
- The IAC hosts a quarterly meeting, connecting faith-based communities with various State and federal law enforcement leadership, including NJOHSP, the Office of the U.S. Attorney for the District of New Jersey, the New Jersey Office of the Attorney General, New Jersey State Police, FBI, prosecutors, and other local law enforcement partners.
- Through the IAC, NJOHSP regularly connects members with vulnerability risk assessment tools and personnel, grant application guidance, suspicious activity reporting briefs, training opportunities, and other resources.
- In December 2022, NJOHSP formed the 14-member IAC Executive Committee, who represent each of New Jersey's major religious communities. The committee functions as a critical resource to IAC members, including law enforcement, seeking to identify and address concerns in their respective communities as well as encouraging cross community collaboration and expertise sharing.

Learn more about the IAC at njohsp.gov/connect/interfaith-advisory-council.

Community Resources

To supplement the key activities of the IAC, NJOHSP provides security resources at no cost and facilitates the availability of grant opportunities for nonprofit organizations in these communities to improve security and develop their own training programs.

Federal Nonprofit Security Grant Program

Provides funding to organizations, as described under section 501(c)(3) of the Internal Revenue Code of 1986, at high risk of terrorist attacks and located within designated areas of New Jersey.

For more information, visit njohsp.gov/grants/federal-nonprofit-security-grant-program.

New Jersey Nonprofit Security Grant Program

Provides funding to eligible nonprofit organizations across New Jersey, as described under section 501(c)(3) of the Internal Revenue Code of 1986, at the greatest risk of terrorist attacks.

For more information, visit njohsp.gov/grants/state-new-jersey-nonprofit-security-grant-program.

New Jersey Shield

New Jersey Shield is a collaboration between the New Jersey Office of Homeland Security and Preparedness (NJOHSP) and the New Jersey Regional Operations and Intelligence Center (NJ ROIC). It is a private–public partnership program that fosters information sharing and strengthens collaboration by enhancing communication between New Jersey State agencies, homeland security representatives, and law enforcement officials, as well as private- and public-sector managers of security, emergency management, and business continuity.

For member eligibility individuals must be a:

- ✓ Federal, State, or local government representative or law enforcement agent tasked with counterterrorism, cybersecurity, or emergency preparedness duties, or
- ✓ Private- and public-sector security director or manager tasked with duties related to their organization's security, emergency management, and business continuity.

New Jersey Shield is a free service that serves as a centralized location for members to obtain counterterrorism, cybersecurity, and emergency preparedness information and resources. This includes a members-only portal that contains:

- Speaker Series Webinars with Subject Matter Experts
- Physical Security Common Vulnerability Monthly Focus Products
- NJOHSP and NJ ROIC Analytical Products and Publications
- Partner Agency Intelligence Products
- Advisories and Alerts
- Training Resources and Upcoming Classes
- Resource Library

New Jersey is home to many organizations that operate on a national and global scale. By partnering with similar programs worldwide as part of a global network, New Jersey Shield meets the needs of its partners not only in New Jersey, but in other states in the U.S. and in countries across the world.

New Jersey Shield's motto is "Working Together to Build a Prepared and Resilient New Jersey." Two-way communication is key to the program's success. Members are asked to participate by reporting suspicious activity, sharing their subject matter expertise and best practices, identifying preparedness and resiliency gaps, and assisting in developing solutions.

To learn more or apply for membership,
please visit our web page at njohsp.gov/connect/new-jersey-shield.

New Jersey Cybersecurity and Communications Integration Cell

The New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) is the state's one-stop shop for cybersecurity information sharing, threat intelligence, and incident reporting. Acting in a cyber fusion center capacity, the NJCCIC is a division within the New Jersey Office of Homeland Security and Preparedness. The NJCCIC works to make New Jersey more resilient to cyberattacks by promoting statewide awareness of cyber threats and widespread adoption of best practices. NJCCIC provide a wide array of cybersecurity services, including the development and distribution of cyber alerts and advisories, cyber tips, and best practices for effectively managing cyber risk. Other services include threat briefings, risk assessments, incident response support, and training.

Information Sharing

We promote shared and real-time awareness of cyber threats for New Jersey's citizens, businesses, local governments, and critical infrastructure owners and operators. By bridging the information divide, we can reduce our state's cyber risk, respond to emerging incidents, and prevent future attacks.

Cyber Threat Analysis

We fuse data from technical and non-technical sources in order to analyze our local cyber threat landscape and educate the public. The information we collect is published across a variety of cyber threat intelligence products using easy-to-understand language.

Incident Reporting

Help us track cyber-related crime by reporting data breaches and other cyber incidents. This data helps us to create alerts and advisories that raise awareness and prevent future incidents.

NJCCIC Membership

An NJCCIC membership enables you to increase your knowledge and awareness, becoming the strongest defense against cyber-attacks. Join today at no cost at cyber.nj.gov/members and the NJCCIC will deliver the latest cyber alerts and advisories to your inbox, along with our bulletins, training notifications, and other important updates.

NJCCIC Cybersecurity Incident Reporting System

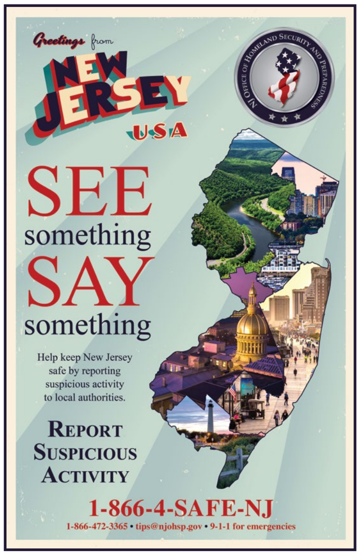
The NJCCIC Incident Reporting System provides a secure, web-enabled means of reporting cybersecurity incidents to the NJCCIC. The information you submit allows us to provide timely handling of your security incident, as well as the ability to conduct improved analysis. If you would like to report a cybersecurity incident, visit cyber.nj.gov/report.

Reporting Suspicious Activity

Suspicious Activity Reporting

The New Jersey Office of Homeland Security and Preparedness (NJOHSP) encourages law enforcement, first responders, and private- and public-sector partners to report potential threats and suspicious activity related to terrorism, targeted violence, counterintelligence, or other related activity. The "See Something, Say Something" campaign benefits families, friends, and neighbors by bringing suspicious behavior to the attention of law enforcement. Reporting suspicious behavior could potentially stop the next terrorist incident. Even if you think your observation is not important, it may be a piece of a larger puzzle.

Public Engagement


Greetings from
NEW JERSEY
USA
NJ Office of Homeland Security and Preparedness
SEE something
SAY something
Help keep New Jersey safe by reporting suspicious activity to local authorities.
Report Suspicious Activity
1-866-4-SAFE-NJ
1-866-472-3365 • tips@njohsp.gov • 9-1-1 for emergencies

The "See Something, Say Something" campaign empowers and educates the public on suspicious activity reporting. In 2021, NJOHSP developed and released two SAR public service announcements (PSAs) designed to educate the public on how to report suspicious activity that may be related to terrorism, targeted violence, counterintelligence, or other related activity and the importance of staying vigilant when surrounded by large groups of people. The community-based video shows how the public plays a key role in reporting suspicious behaviors to law enforcement. The school-focused PSA is a "challenge video" that includes a "what would you do" scenario, which is aimed at middle and high school-aged children to help identify school threats. Both videos stress the importance of recognizing potential indicators in thwarting potential incidents.

Suspicious activity reports have led to investigations that thwarted several terrorist plots in the tri-state area. Read the New Jersey Suspicious Activity Reporting Success Stories to learn how these reports helped detect and deter possible attacks.

Information Sharing

The New Jersey Suspicious Activity Reporting System (NJSARS) shares suspicious activity related to terrorism, targeted violence, counterintelligence, or other criminal activity to law enforcement partners throughout the State. NJSARS is linked to the FBI's national suspicious activity reporting (SAR) system known as eGuardian, which is a part of the Nationwide SAR Initiative. The partnership forms a single repository accessible to thousands of law enforcement personnel and analysts nationwide.

Report Suspicious Activity

SARs with a possible nexus to terrorism, targeted violence, or other criminal activity should be reported immediately, per existing protocols. Activity can also be reported 24/7 to NJOHSP's Counter-Threat Watch Unit via the following:

☎ **1-866-4-SAFE-NJ (866-472-3365)**

✉ tips@njohsp.gov

www njohsp.gov/threat-landscape/report-suspicious-activity

Glossary

Glossary

Abortion-Related Extremists (AREs) – Individuals or groups who justify violence against people and establishments representing opposing views on abortion. AREs advocate for violence, death threats, and other criminal activity to include arson, vandalism, and harassment against women's reproductive healthcare facilities and medical professionals.

Active Clubs – Decentralized white racially motivated extremist (WRME) network of combat sports groups where individuals can organize physical training, radicalize, and mobilize to conduct acts of violence.

Advanced Persistent Threats (APT) – An adversary that possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat:

(i) pursues its objectives repeatedly over an extended period of time;

(ii) adapts to defenders' efforts to resist it; and

(iii) is determined to maintain the level of interaction needed to execute its objectives.

Adversary – Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

Alternative Social Media Platforms – Created as an alternative for mainstream social media, these platforms focus on opposition to free speech restrictions and generally offer less content moderation as well as increased encryption.

Al-Qa'ida (AQ) – An Islamist extremist organization founded in 1988 by Usama bin Ladin and other Arab foreign fighters who fought against the Soviet Union in Afghanistan in the 1980s. It provides religious authority and strategic guidance to its followers and affiliated groups.

Al-Qa'ida in the Arabian Peninsula (AQAP) – An Islamist extremist organization based in Yemen. It is al-Qa'ida's most prominent global affiliate.

Al-Qa'ida Network – A decentralized organization that relies on social ties and local relationships to share resources among the affiliates.

Al-Shabaab – An Islamist extremist organization founded in 2006 that seeks to establish an austere version of Islam in Somalia. The group pledged allegiance to al-Qa'ida in February 2012. Since late 2018, the group has clashed with the rival ISIS group, which has a branch in Somalia.

Analysis – The examination of acquired data for its significance and probative value to the case.

Anarchist/Anti-Fascist Extremists – Believe that society should exist absent of "oppressive" governments, laws, law enforcement, or any other authority. They will use violence or criminal activity to oppose what they perceive as fascist, racist, or sexist injustices and organizations.

Animal Rights Extremists – Believe all animals—human and non-human—have equal rights of life and liberty and are willing to inflict economic damage on individuals or groups to advance this ideology.

Anti-Government Extremists – Believe the U.S. political system is illegitimate and force is justified to bring about change. Additionally, this includes individuals who do not necessarily question the legitimacy of government but express their opposition to specific policies, entities, officials, and political parties through threats or acts of violence. This can include militia extremists and sovereign citizen extremists.

Artificial Intelligence (AI) – (1) A branch of computer science devoted to developing data processing systems that performs functions normally associated with human intelligence, such as reasoning, learning, and self-improvement. (2) The capability of a device to perform functions that are normally associated with human intelligence such as reasoning, learning, and self-improvement.

Attack – An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity.

Attack Surface – The set of points on the boundary of a system, a system component, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, component, or environment.

Black Racially Motivated Extremists (BRMEs) – Believe in and/or advocate for the advancement of the black race over all others and use violence or criminal activity to further their ideology. The intent and capability of BRMEs varies by organization and region. The majority of BRME organizations focus their efforts on spreading extremist rhetoric to recruit new members.

Bot – Automated account that executes specific tasks such as publishing, sharing, and resharing content.

Breach of Security – "Breach of security" means unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable. Good faith acquisition of personal information by an employee or agent of the business for a legitimate business purpose is not a breach of security, provided that the personal information is not used for a purpose unrelated to the business or subject to further unauthorized disclosure.

Control – A means of managing a risk or ensuring that an objective is achieved. Controls can be preventative, detective, or corrective and can be fully automated, procedural, or technology-assisted human-initiated activates. They can include actions, devices, procedures, techniques, or other measures.

Counterintelligence – Activities designed to prevent or thwart an enemy or other foreign entity from spying, intelligence gathering, and sabotage. Counterintelligence involves understanding and neutralizing intelligence operations and activities, regardless of industry.

Critical Infrastructure – System and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. [Critical Infrastructures Protection Act of 2001, 42 U.S.C. 5195c(e)]

Cyberattack – An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

Cyber Incident – Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein. See Incident.

Deepfake – Synthetic media generated or manipulated using artificial intelligence (AI) to superimpose faces, insert new individuals or items, modify behavior, or change audio and dialogue.

Distributed Denial-of-Service – A Denial-of-Service technique that uses numerous hosts to perform the attack.

Domestic Terrorism – Violence committed by individuals or groups primarily associated with U.S.-based movements, including anti-government, race-based, religious, and single-issue extremist ideologies.

Encrypted Messaging Applications – Applications that offer end-to-end encryption of communications which promote privacy as only the intended recipient(s) of a message or contents can view it.

Environmental Extremists – View manmade threats to the environment as so severe that violence and property damage are justified to prevent further destruction.

Generative Artificial Intelligence (GenAI) – A type of AI that creates new content, like text, images, or videos, by learning from existing data patterns.

HAMAS – HAMAS, an acronym for Harakat al-Muqawama al-Islamiyya, or the "Islamic Resistance Movement," founded in 1987, is an offshoot of the Palestinian Muslim Brotherhood that aims to remove Israel and replace it with a Palestinian Islamic state.

Hizballah – Arabic for "Party of God," the group is a Lebanon-based, Iranian-backed Shiite political party and paramilitary group that maintains a regional military force and an external attack-planning component known as the Islamic Jihad Organization (IJO).

Homegrown Violent Extremists (HVEs) – Individuals inspired—as opposed to directed—by foreign terrorist organizations and radicalized in the countries in which they are born, raised, or reside.

Industrial Control System (ICS) – General term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC) found in the industrial sectors and critical infrastructures. An industrial control system consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy).

ISIS – Salafi-jihadist militant group that split from al-Qa'ida in 2014 and established its self-proclaimed "caliphate," claiming authority over all Muslims. ISIS is also referred to as the Islamic State of Iraq and Syria, the Islamic State of Iraq and the Levant, the Islamic State, or Daesh.

Malware – A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.

Militia Extremists – View the federal government as a threat to the rights and freedoms of Americans. They judge armed resistance as necessary to preserve these rights and justify the use of violence to counter perceived threats to, or violations of, the U.S. Constitution.

Operational Technology – The use of computers to monitor or alter the physical state of a system, such as the control system for a power station or the control network for a rail system. The term has become established to demonstrate the technological and functional differences between traditional IT systems and Industrial Control Systems environment.

Paste Site – A website that allows users to store and share text-based information, such as code snippets, scripts, configuration files, or any other form of plain text.

Phishing – Tricking individuals into disclosing sensitive personal information through deceptive computer-based means.

Risk – The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.

Salafi-jihadism – An extreme interpretation of Islam to which multiple foreign terrorist organizations and individuals adhere.

Sensitive Personally Identifiable Information (SPII) – Personal information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

Single-Issue Extremists – Participate in violence stemming from domestic, political, or economic issues. This includes animal rights, environmental, and abortion-related extremists.

Soft Targets – Easily and publicly accessible locations which have limited security or protective measures.

Sovereign Citizen Extremists – View federal, state, and local governments as illegitimate to justify their violence and other criminal activity. They assert they are not subject to questioning or arrest by law enforcement, paying taxes or fines, complying with summonses, or possessing official licenses.

Terrorism – The unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

Threat – Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Unauthorized Access – Occurs when a user, legitimate or unauthorized, accesses a resource that the user is not permitted to use.

Vulnerability – Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

White Racially Motivated Extremists (WRMEs) – Believe in and/or advocate for the advancement of the white race over all others, and use violence or criminal activity to further their ideology. WRMEs will likely leverage a diverse network of online platforms to disseminate strategic and tactical guidance, encourage violence, and share propaganda to motivate followers to conduct attacks, engage in vandalism, and intimidate minorities.

NJ Office of Homeland Security and Preparedness

Recognize and Report

Potential Threats and Suspicious Activity

Expressed or Implied Threat: Threatening to commit a crime that could harm or kill people or damage a facility, infrastructure, or secured site

Surveillance: A prolonged interest in or taking pictures/videos of personnel, facilities, security features, or infrastructure in an unusual or covert manner

Theft/Loss/Diversion: Stealing or diverting items—such as equipment, uniforms, or badges—that belong to a facility or secured site

Breach/Attempted Intrusion/Trespassing: Unauthorized people trying to enter a restricted area or impersonating authorized personnel

Testing Security: Probing or testing a facility's security or IT systems to assess the strength or weakness of the target

Aviation Activity: Operating or interfering with the operation of an aircraft that poses a threat of harm to people and property

Acquiring Expertise: Gaining skills or knowledge on a specific topic, such as facility security, military tactics, or flying an aircraft

Eliciting Information: Questioning personnel beyond mere curiosity about an event, facility, or operations

Misrepresentation: Presenting false information or misusing documents to conceal possible illegal activity

Cyber Attack: Disrupting or compromising an organization's information technology systems

Recruiting: Attempting to recruit or radicalize others by providing tradecraft advice or distributing propaganda materials

Financing: Providing direct financial support to operations teams and contacts, often through suspicious banking/financial transactions

Sabotage/Tampering/Vandalism: Damaging or destroying part of a facility, infrastructure, or secured site

Material Acquisition/Storage: Acquisition and/or storage of unusual quantities of materials, such as cell phones, radio controllers, or toxic materials

Weapon Collection/Storage: Collection or discovery of unusual amounts of weapons, including explosives, chemicals, or other destructive materials

Report Suspicious Activity

1-866-4-SAFE-NJ (866-472-3365)