2026
THREAT ASSESSMENT

NEW JERSEY OFFICE OF HOMELAND SECURITY AND PREPAREDNESS

About NJOHSP

The New Jersey Office of Homeland Security and Preparedness (NJOHSP) was established in 2006 to administer, coordinate, lead, and supervise New Jersey's counterterrorism and preparedness efforts across all levels of government. As the State's central coordinating agency for homeland security, NJOHSP works closely with federal, State, county, and local partners—as well as nonprofit organizations, academic institutions, and the private sector—to safeguard New Jersey's residents, infrastructure, and institutions.

NJOHSP's mission has expanded significantly as the threat environment has evolved. In 2015, the creation of the New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) formalized the State's leadership role in cybersecurity information sharing, cyber incident reporting, election security, and statewide cyber defense. By 2023, NJOHSP further broadened its mission by integrating statewide counterintelligence functions to confront the increasing threat posed by hostile foreign intelligence activity, espionage, cyber-enabled intelligence operations, and transnational repression.

In 2025, Governor Murphy signed Executive Order 404 which reaffirmed and modernized NJOHSP's authorities, formally designating the Office as New Jersey's lead agency for counterterrorism, counterintelligence, cybersecurity, and related preparedness efforts. The order strengthened intergovernmental coordination, unified statewide homeland security responsibilities, and aligned the Office's authorities with emerging and modern threats.

Today, NJOHSP's capabilities span the full spectrum of homeland security disciplines—counterterrorism, targeted violence prevention, counterintelligence, cybersecurity, preparedness, and administrative support. Through a whole-of-state approach that integrates local, county, State, federal, nonprofit, and private-sector partners, NJOHSP enhances New Jersey's ability to anticipate, disrupt, withstand, and respond to evolving threats, ensuring the safety, security, and resilience of all who live, work, and visit here.

Mission

To lead and coordinate all homeland security issues and efforts, including counterterrorism, counterintelligence, cybersecurity, preparedness, and resiliency across all levels of government, law enforcement, and the private sector.

Vision

A safe, secure, and resilient New Jersey where acts of terrorism, targeted violence, cyberattacks, and hostile foreign intelligence activity are anticipated, detected, and prevented through unified statewide action and whole-of-state collaboration.

Core Values

SERVICE — We are guided by a shared commitment to service, always putting the state of New Jersey and its residents first, with mission before self. Our work is defined by timeliness, agility, and relevance.

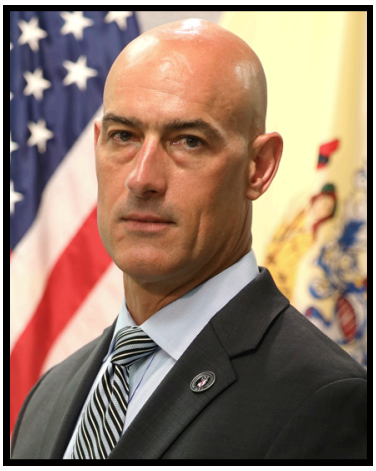
TEAMWORK — We believe in teamwork, standing with and behind one another, and recognizing that strong partnerships—both internal and external—are essential to achieving success. We understand that our mission cannot be accomplished alone.

EXCELLENCE — We strive for excellence in everything we do, taking great pride in the quality of our work and committing ourselves to perform every task, project, and initiative to the best of our ability.

DIVERSITY — We are committed to building a workforce that reflects the diversity of New Jersey's population, and we actively foster diversity of thought, perspective, and problem-solving.

INTEGRITY — Above all, we uphold integrity, holding ourselves to the highest moral and ethical standards in both our personal and professional lives. We are dedicated to acting with honor and truthfulness and earning the trust placed in us.

Foreword



The New Jersey Office of Homeland Security and Preparedness (NJOHSP) plays a crucial role in safeguarding the state, as well as its residents, visitors, businesses, and diverse communities through proactive security and preparedness strategies. We will continue our seamless collaboration with federal, State, county, and local partners, as well as with emergency managers, first responders, private-sector, and community organizations, ensuring New Jersey remains prepared, protected, and resilient.

As we move forward in 2026, we recognize the transformative impact of Executive Order No. 404 signed in 2025. This landmark order has modernized and clarified our responsibilities, establishing NJOHSP as New Jersey's primary lead in counterterrorism, counterintelligence, cybersecurity, and preparedness—strengthening our ability to protect the state, its residents, and the institutions that uphold our democracy with foresight, integrity, and unity of purpose.

Our commitment to counterterrorism remains steadfast as we adapt strategies to address global and domestic extremism. Ongoing collaboration and intelligence-sharing with local, State, and federal agencies will enable us to anticipate and effectively prevent threats. Counterintelligence is equally crucial for protecting our state's sensitive information and infrastructure, where we focus on thwarting activities that threaten national interests using advanced technology and strategic alliances.

Cybersecurity is a top priority given the increasing complexity and frequency of cyber threats. We are investing in cutting-edge technologies and training programs to bolster our defenses, ensuring the protection of critical infrastructure and personal data as we navigate the evolving digital landscape.

As we look toward major upcoming events such as the United States' Semiquincentennial celebrations, FIFA World Cup 2026, and Sail4th 250, we will accelerate our preparedness and planning efforts to manage the global attention and coordination these events demand. As one of the host states and home to the World Cup final, New Jersey will attract thousands of visitors, including teams, officials, and fans from around the world, necessitating an exceptional level of coordination and planning. NJOHSP is committed to comprehensive planning and intelligence-sharing for the nation's 250th anniversary, ensuring effective threat response. For Sail4th 250, NJOHSP will collaborate with the U.S. Coast Guard and maritime partners to secure New Jersey's waterways.

On behalf of NJOHSP and its staff, we thank all our partners who contributed to the 2026 Threat Assessment. We encourage everyone to stay alert and remember: if you "See Something, Say Something." Report suspicious activity that may be connected to terrorism, targeted violence, counterintelligence threats, or other concerning behavior to your local law enforcement agency or to NJOHSP's Counter-Threat Watch Unit at 866-4-SAFE-NJ and tips@njohsp.gov.

Sincerely,

Thomas G. Hauck

Thomas G. Hauck
Director
January 2026


NJ Office of Homeland Security and Preparedness

Table of Contents

Glossary

To view a glossary of terms mentioned throughout this Threat Assessment, please go to njohsp.gov/threat-landscape/threat-assessment/glossary, or scan or click the QR code.

Executive Summary

The New Jersey Office of Homeland Security and Preparedness assesses that, in 2026, homegrown violent extremists (HVEs) and white racially motivated extremists (WRMEs) represent the highest terrorist threats to New Jersey. Moderate terrorist threats include anarchist/anti-fascist, anti-government, and sovereign citizen extremists, as well as pro-choice and pro-life extremists. Low terrorist threats include al-Qa'ida and its affiliates; animal rights, Black racially motivated, environmental, and militia extremists; HAMAS; Hizballah; and ISIS.

In 2025, New Jersey authorities disrupted multiple terrorism-related plots and material support activities, including the arrest of three local individuals involved in threatening communications and support for ISIS. At the same time, al-Qa'ida and ISIS and their supporters released propaganda in the form of publications and videos praising past attackers and urging U.S.-based sympathizers, including those in New Jersey, to carry out acts of violence. Together, these developments underscore a threat environment in which foreign terrorist organizations (FTOs) seek to radicalize and mobilize HVEs on their behalf.

What is an HVE?

HVEs are individuals inspired—as opposed to directed—by foreign terrorist organizations and radicalized in the countries in which they are born, raised, or reside.

While HVEs most frequently support ISIS, reporting in New Jersey since the start of the Israel–HAMAS conflict on October 7, 2023, indicates a slight increase in references to individuals alleged to express support for HAMAS. Local expressions of support further illustrate how international events and messaging associated with FTOs have influenced discourse within the state, even as overall activity levels remain low.

In 2026, WRMEs will primarily engage with supporters online to spread their extremist messages while inspiring others to commit violence on behalf of their ideology. A review of approximately 1,200 pieces of propaganda material found in New Jersey from 2019 through 2025 showed how extremists with various ideologies, including WRMEs, seek to promote their beliefs and disparage those with opposing views. These individuals used a variety of images and symbols to promote their ideology and displayed the materials on public infrastructure.

What is Domestic Terrorism?

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.

Nihilistic violent extremist (NVE) groups, including predatory online communities such as 764 and CVLT (pronounced cult), target juveniles through sexual exploitation and by encouraging self-harm. NVEs have been present within New Jersey, using known 764 and CVLT tactics to coerce victims through social media, gaming platforms, and smart phone applications to produce child sexual abuse material and other harmful violent content. Many NVE subgroups adhere to WRME ideology, neo-Nazism, accelerationism, satanism, and other cult-like subcultures.

What is an NVE?

Individuals who use violence or criminal activity in furtherance of political, social, or religious goals that derive primarily from a hatred of society and a desire to bring about its collapse by sowing indiscriminate chaos, destruction, and social instability.

HVEs and domestic extremists leverage social media and encrypted messaging platforms to spread propaganda, radicalize and mobilize supporters, coordinate attacks, and advance their objectives. In 2025, individuals adhering to various extremist ideologies exploited social media for preoperational activities, particularly related to radicalization and recruitment, to target users with tailored narratives. As social media and online technology evolve, extremists have readily adapted their tactics to capitalize on these developments.

HVEs and domestic extremists target a range of critical infrastructure sectors in furtherance of various ideologies to cause widespread disruption of key systems. In 2025, individuals in New Jersey communicated explicit or implied threats to intimidate religious communities, houses of worship, and faith-based institutions. New Jersey also saw an uptick in reporting against the Government Services and Facilities sector and the Healthcare and Public Health sector, indicating national events and personal grievances may be inspiring individuals to plot against these sectors in the state.

Nation-state actors and individuals acting on behalf of foreign governments leverage strategies such as cyber intrusions and attacks, espionage, and theft to actively target critical infrastructure and circumvent laws in pursuit of economic and military advantage over the U.S. New Jersey's strategic location, dense network of critical infrastructure, and significant concentration of sensitive technological industries, financial institutions, and academic research centers make it an attractive target for foreign intelligence entities and nation-state actors.

Foreign adversaries, particularly the People's Republic of China, Russia, and Iran, routinely engage in intelligence-gathering activities aimed at undermining U.S. economic and national security. These governments deploy a variety of tactics including stealing sensitive proprietary information, pre-positioning themselves within the networks of U.S.-based critical infrastructure, and conducting transnational repression operations in New Jersey to harass, surveil, and coerce expatriates to return to their home country to face criminal prosecution.

The New Jersey Cybersecurity and Communications Integration Cell assesses with high confidence that in 2026 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 residents, the economy and public interests of the state, and national security. The 2026 threat landscape presents unprecedented challenges across multiple dimensions, including nation-state threats, cybercrime threats, and emerging trends, such as artificial intelligence (AI)-orchestrated attacks. Sophisticated threat actors, AI-powered attack tools, systemic vulnerabilities, and reduced federal support require enhanced State and local cybersecurity investment, collaboration, and vigilance.

Major events and mass gatherings, such as the upcoming FIFA World Cup 2026 and Sail4th 250, continue to face a heightened threat environment as evidenced by recent attacks, disrupted plots, and propaganda releases from a variety of violent extremist movements. These high-profile events, which will draw large crowds from around the world, can also be potential targets of disruptive or otherwise criminal actions, including physical assault, harassment, intimidation, vandalism, and property damage.

2026 Assessed Threat Rankings

HIGH THREAT

HOMEGROWN VIOLENT EXTREMISTS	DOMESTIC
WHITE RACIALLY MOTIVATED EXTREMISTS	DOMESTIC

MODERATE THREAT

ANARCHIST/ANTI-FASCIST EXTREMISTS	DOMESTIC
ANTI-GOVERNMENT EXTREMISTS	DOMESTIC
PRO-CHOICE AND PRO-LIFE EXTREMISTS	DOMESTIC
SOVEREIGN CITIZEN EXTREMISTS	DOMESTIC

LOW THREAT

AL-QA'IDA AND AFFILIATES	INTERNATIONAL
ANIMAL RIGHTS EXTREMISTS	DOMESTIC
BLACK RACIALLY MOTIVATED EXTREMISTS	DOMESTIC
ENVIRONMENTAL EXTREMISTS	DOMESTIC
HAMAS	INTERNATIONAL
HIZBALLAH	INTERNATIONAL
ISIS	INTERNATIONAL
MILITIA EXTREMISTS	DOMESTIC

Detailed information on these extremist groups and ideologies can be found at njohsp.gov.


NJ Office of Homeland Security and Preparedness

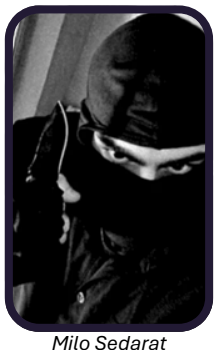
COUNTERTERRORISM

HVEs in New Jersey Mobilize Amid Global FTO Propaganda and Messaging

In 2025, authorities in New Jersey disrupted multiple plots and material support efforts, while ISIS and al-Qa'ida released publications praising past attackers and encouraging U.S.-based sympathizers to engage in violence. Recent local homegrown violent extremist (HVE) cases and intensified propaganda from ISIS and al-Qa'ida highlight a threat environment where local foreign terrorist organization (FTO) supporters seek to mobilize as global messaging urges violence in the U.S., including in New Jersey.

NOV 2025

Tomas-Kaan Jimenez-Guzel



Milo Sedarat

Authorities arrested Tomas-Kaan Jimenez-Guzel and Milo Sedarat, both of Montclair (Essex County), on related matters, with Jimenez-Guzel charged in connection with ISIS-inspired activity and Sedarat charged for making violent antisemitic threats. Both were allegedly in communication with individuals who expressed ISIS ideology, discussed traveling overseas to fight for the group, and desired to engage in violence. Law enforcement arrested Sedarat at his home and Jimenez-Guzel at the Newark Liberty International Airport as he attempted to travel to Syria to join ISIS.

MAR 2025

Kyse Abushanab, of Budd Lake (Morris County), pleaded guilty to concealing material support and resources for a designated FTO. According to court documents, between March 2021 and January 2022, Abushanab compiled resources regarding the manufacture and use of weapons of mass destruction with the intention of providing them to ISIS. The resources included videos and documents with step-by-step instructions for making explosive devices and their components. Abushanab used encrypted applications and untraceable email accounts to conceal his support of ISIS from law enforcement.

ISIS and al-Qa'ida Propaganda Efforts Seek to Inspire HVEs

Since June 2025, al-Qa'ida in the Arabian Peninsula and its followers have released four publications exploiting perceived U.S. instability and admonishing Western governments. Each publication praises past attackers to shame perceived inaction among sympathizers and seeks to inspire renewed commitment. One publication encouraged supporters, including those in New Jersey, to take violent action on behalf of the group.

In May 2025, ISIS released a video calling on supporters worldwide to target Jewish individuals and institutions beyond the Palestinian territories, citing embassies in the U.S. and Europe as viable targets. The video, which was also referenced in *al-Naba*, the group's weekly Arabic-language newsletter, claimed these "global operations" as "essential" to its broader strategy.

Two Years Post Israel-HAMAS Conflict: Impacts to New Jersey

Since the onset of the Israel-HAMAS conflict on October 7, 2023, New Jersey has experienced a modest but noticeable increase in reporting involving alleged HAMAS supporters, indicating that HAMAS propaganda is influencing local perceptions and encouraging rhetoric linked to violent action. The U.S. government designated HAMAS as a foreign terrorist organization (FTO) in 1997 due to its enduring campaign of violence and terror, which involved intimidating, coercing, and attacking civilian populations. Local support for HAMAS highlights how events in the Middle East and FTO propaganda have affected conditions in the state, even as overall activity levels remain low.

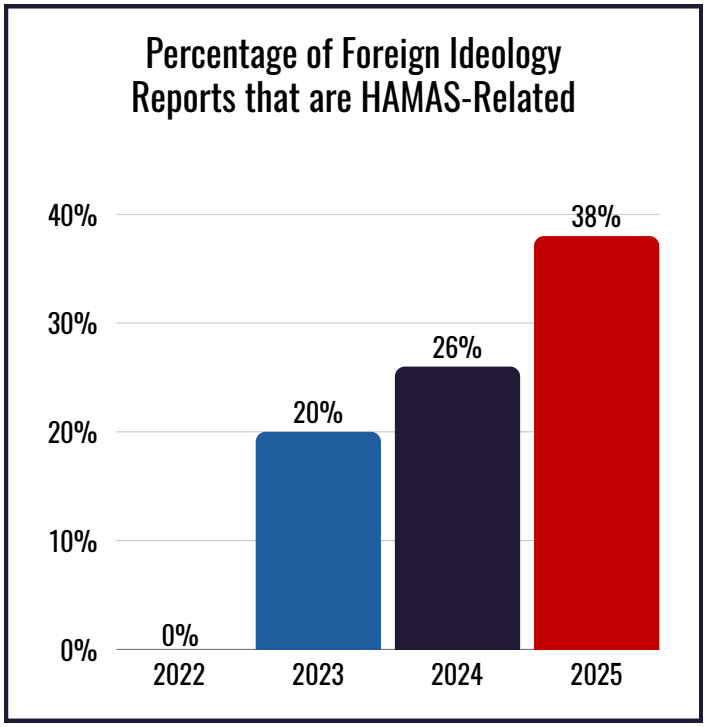
The Role of FTO Propaganda

FTOs publish propaganda or make official statements to encourage supporters globally to act on their behalf. This desired action can be anything from protests to attacks on perceived enemies.

At the onset of the conflict, HAMAS issued messaging encouraging supporters globally to engage in activities supporting its conflict with Israel, including calls for global "days of jihad." HAMAS-affiliated media channels promoted the use of a red triangle pointed-down as a symbol for individuals to demonstrate support for the group. In 2024, around the one-year anniversary of the conflict, HAMAS continued its messaging, calling for "mass activities" in all "Arab, Islamic, and International streets, cities, and capitals."

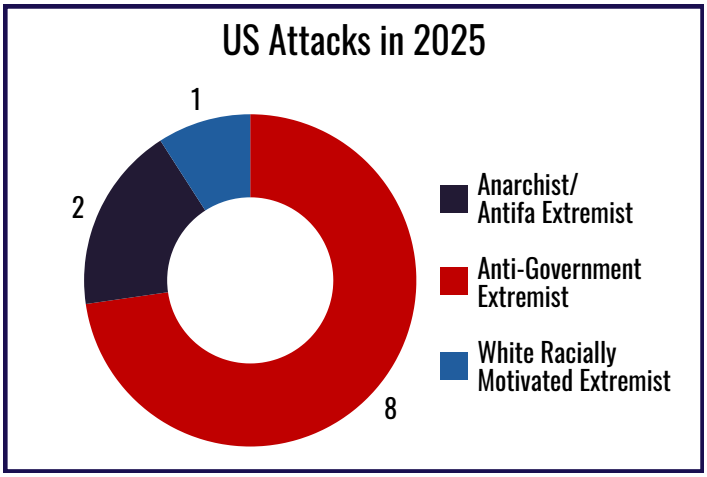
Since October 2023, New Jersey has seen an uptick in reporting concerning individuals supporting HAMAS and encouraging the targeting and killing of members of the Jewish community. Tactics included using the red triangle pointed-down symbol as a way of emphasizing which individuals to target, or phoning perceived Jewish individuals and espousing violent rhetoric at them.

Some reports also highlighted individuals intentionally showing support for HAMAS in predominately Jewish neighborhoods, or stockpiling weapons while making antisemitic remarks and praising HAMAS. A report in August 2024 alleged a New Jersey individual posted messaging online expressing their desire to become a "terrorist," support the "Intifada," and mourned the death of a notable HAMAS leader.



Examining Incidents of Domestic Extremism Nationally

A New Jersey Office of Homeland Security and Preparedness review of 2025 nationwide incidents revealed approximately 39 individuals with a personal grievance and a nexus to a domestic extremist ideology that acted independently or with one or more co-conspirators to conduct 34 incidents. These 39 extremists conducted 11 attacks, 14 threats, and nine plots. Among these individuals more than half targeted elected officials and law enforcement officers, closely mirroring last year's incidents directed at these two sectors.



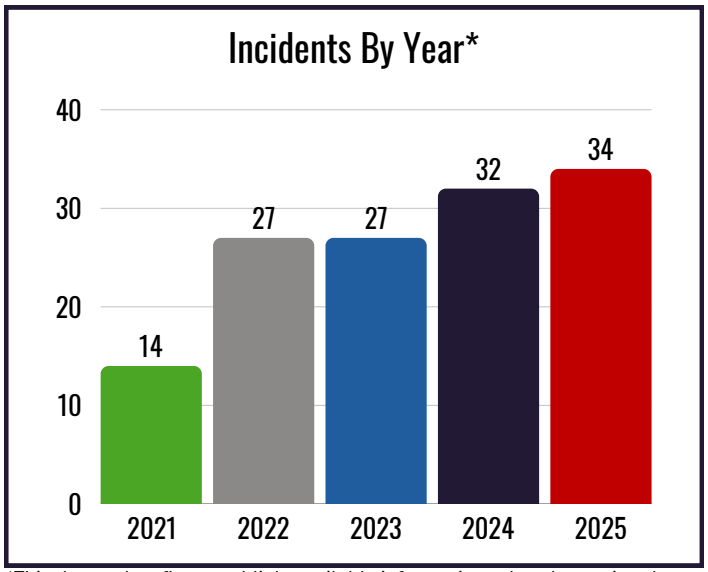
Among the 11 attacks in 2025, extremists with varying ideologies conducted six unrelated acts of violence using a firearm to kill one elected official and spouse at their residence, one law enforcement officer, and three civilians, while wounding approximately 13 others. The remaining five separate incidents consisted of individuals conducting non-fatal arson attacks using homemade incendiary devices to target and vandalize three political offices in separate states, a federal building, and the Pennsylvania governor's mansion.

AUG 2025

Authorities charged Kevin O'Neal, of Tennessee, with 11 counts of attempted first-degree murder of nine detectives and deputies. Officers initially sought to locate O'Neal in connection with arrest warrants for threatening to kill public officials and law enforcement. After apprehending O'Neal, officers noticed an improvised explosive device (IED) smoldering inside his home. Authorities found additional IEDs and determined O'Neal allegedly attempted to detonate the IEDs when officers arrived to arrest him.

JUL 2025

Authorities arrested Nathan Henderson in San Antonio, Texas, after receiving credible information that he expressed a desire to kill black and Jewish individuals along with unnamed government officials using homemade explosive devices. During a search of his home, authorities discovered multiple firearms and ammunition, chemicals associated with homemade explosive devices, 24 grenades, a remote detonator, and approximately 100 metal cylinders intended for blasting caps. Officers also discovered notebooks containing extremist ideology and vague plans to target public venues.

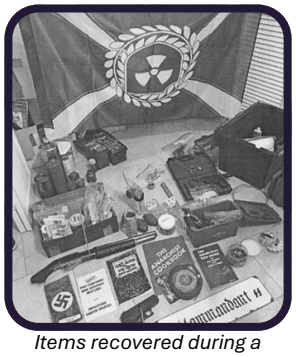


**This data only reflects publicly available information related to national incidents committed by individuals with a clear identifiable nexus to a domestic extremist ideology and may be subject to change.*

WRMEs Leverage Online Support

White racially motivated extremists (WRMEs) will primarily engage with supporters online to spread their extremist messages while inspiring others to commit violence on behalf of their ideology. In 2025, there were eight national incidents involving individuals who adhere to WRME ideology that engaged in various threats and plots and one attack.

NOV 2025



Items recovered during a search of Temple's home.

Federal law enforcement arrested Lucas Temple in Sarasota, Florida, for his alleged ties with numerous extremist groups on the encrypted messaging app Signal. Temple allegedly used multiple aliases on the app to circulate graphic content, detailed instructions for making explosives, violent neo-Nazi propaganda, and a plan to livestream an attack. A search of his home revealed an illegal sawed-off shotgun, a hand-drawn diagram of a homemade detonator, and various pieces of Nazi literature. Temple allegedly posted a manual filled with WRME rhetoric and participated in chats that included graphic discussions.

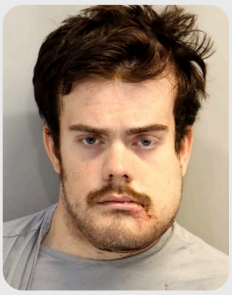
JUL 2025

Authorities in California charged Noah Lamb in connection with a hit list of "high value targets" for assassination, which included U.S. officials, nongovernmental organizations, and leaders of private companies. Lamb was allegedly a member of the Terrorgram Collective, a collection of WRME transnational channels on the encrypted messaging platform Telegram. According to the indictment, Lamb collaborated with members of Terrorgram to strategically choose targets based on the group's belief that "the white race is superior" and that each target had a "list card," which supposedly included reasons the group viewed them as an enemy.

JAN 2025

Authorities arrested Matthew Scouras in Beverly, Massachusetts, after he allegedly posted threats to rape Jewish women on an internet image board and encouraged other users to shoot individuals outside of synagogues. Following a search of his home, authorities recovered more than $70,000 in cash, a Nazi flag, boxes of ammunition, numerous firearms parts, and several guns, including a 9mm Glock "ghost gun."

Online Activity Escalates to Violence



Phoenix Ikner

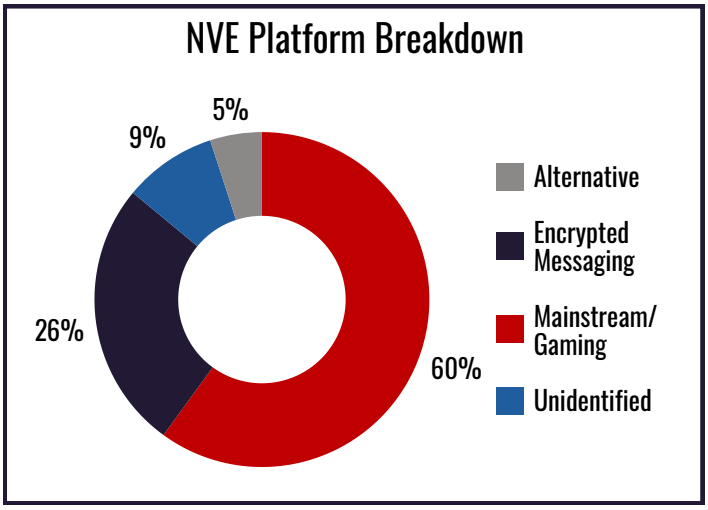
According to authorities, on April 17, 2025, Phoenix Ikner conducted an attack at Florida State University in Tallahassee, killing two individuals and injuring six others. After the attack, authorities located an AR-15-style rifle inside the vehicle he drove to campus along with a .45 caliber pistol and a shotgun recovered at the scene. Ikner's online profiles revealed admiration of Adolf Hitler, Nazis, and various WRME imagery, which included the logo of a group affiliated with WRME ideology. Ikner's former classmates described him as expressing "concerning rhetoric" and said he was asked to leave a political discussion group due to his alleged extremist views.

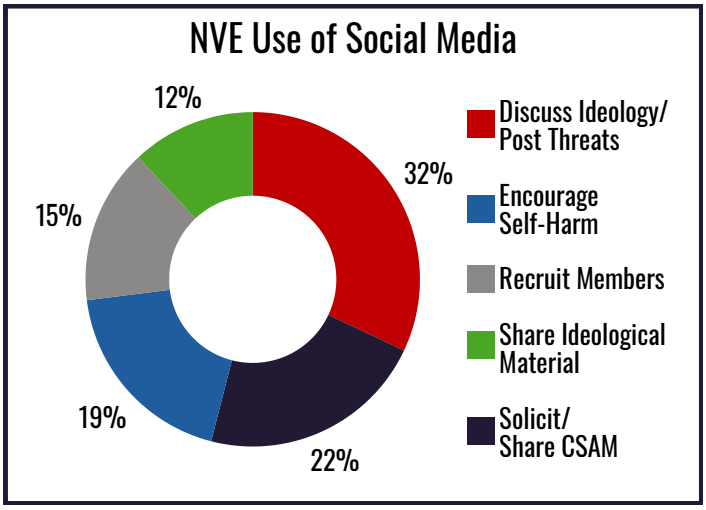
NVE Groups Exploit Vulnerable Juveniles Online

Nihilistic Violent Extremist (NVE) groups, including the 764 network and CVLT (pronounced cult), target juveniles online through sexual exploitation and encouragement of self-harm. NVEs have been present within New Jersey, using known 764 and CVLT tactics to coerce victims through social media, gaming platforms, and smart phone applications to produce child sexual abuse material (CSAM) and other harmful violent content. Many NVE subgroups adhere to WRME ideology, neo-Nazism, accelerationism, satanic rituals, and other cult-like subcultures.

NVEs primarily operate through online platforms like Telegram, Discord, and Roblox, which allow groups to target minors with limited moderation, often using coded language such as "Cheese Pizza," that can refer to child pornography without overtly highlighting it to avoid automated content moderation. Additionally, NVEs often use monikers to mask their identity while operating on behalf of the group. These groups typically post black and white graphics, edits of gore, animal abuse, suicide, or sexual violence in a meme-like style. Online users adhering to NVE ideology often have a fixation on violent, extremist, or nihilistic topics such as neo-Nazism, school shootings, serial killers, occultism, and conspiracy theories.

A New Jersey Office of Homeland Security and Preparedness review of open-source NVE incidents in 2025 revealed that a majority of NVE suspects (79 percent) were between the ages of 18 and 29. These subjects primarily target their victims on mainstream and gaming platforms (60 percent) to discuss ideology or post threats (32 percent) and solicit/share CSAM (22 percent).





New Jersey Case Study

In November 2025, authorities arrested Marek Cherkaoui, 21, of Egg Harbor Township (Atlantic County), for his connection to the 764 network. According to the indictment, Cherkaoui allegedly used online platforms to threaten a minor, engage in doxxing, express support for mass shooters, solicit CSAM, and encourage individuals to harm themselves and others. Cherkaoui allegedly posted a link to a "Power Grid Sabotage Manual" on Telegram as a part of the Terrorgram Collective and purchased books regarding the manufacture of explosives, as well as body armor, zip ties, a trench coat, ski masks, and tactical gear. During a search of Cherkaoui's home, authorities found writings which included a multi-step plan that involved joining ISIS and returning to the U.S. to commit acts of terrorism.

Domestic and Homegrown Violent Extremist Use of Social Media

In 2026, extremists will likely exploit social media, often using mainstream sites to target broader audiences and direct them toward more niche and encrypted online platforms, further propagating extremist ideologies in spaces with less content moderation and increased data security. In 2025, individuals adhering to various extremist ideologies exploited social media for preoperational activities, particularly related to radicalization and recruitment, and leveraged mainstream, alternative, and encrypted platforms to target users with tailored narratives. As social media and online technology evolve, extremists have readily adapted their tactics to capitalize on these developments. In New Jersey, domestic extremist and homegrown violent extremist (HVE) online activity closely mirror trends seen nationwide, with individuals leveraging a mix of mainstream and encrypted platforms for various preoperational activities.

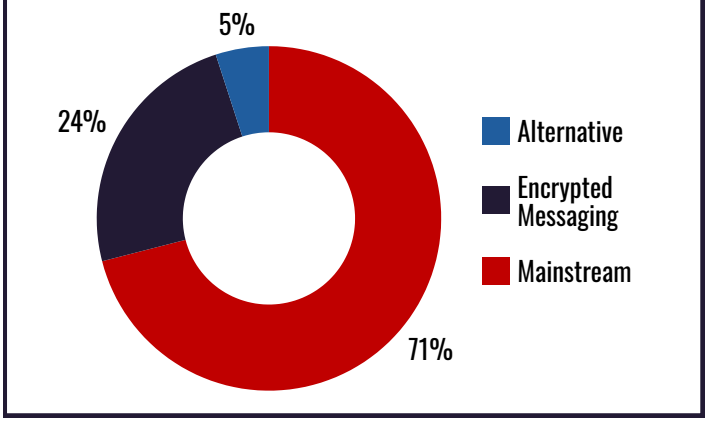
Domestic Extremists

Twenty of the 34 domestic extremist attacks, plots, and threats had a social media nexus, with 25 individuals across these incidents adhering mainly to anti-government ideology, followed by white racially motivated and anarchist/anti-fascist extremism. These individuals continued to rely on mainstream platforms to fuel their preoperational online activity, using these platforms to discuss their ideologies and post threats, which accounted for 55 percent of their online activity.

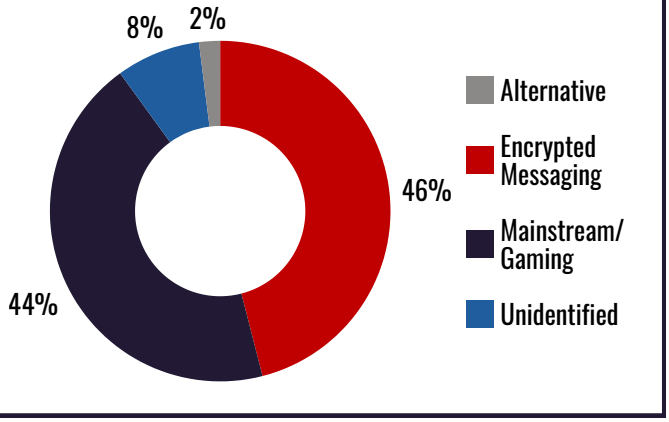
Homegrown Violent Extremists

The 19 identified HVE attacks, plots, and threats mainly drew inspiration from ISIS, accounting for 18 of the 19 related incidents. HVEs exploited encrypted messaging applications in 46 percent of cases, followed by mainstream platforms in 44 percent of the identified cases. They primarily used social media to discuss ideology and post threats (30 percent), followed by viewing propaganda and ideological material (23 percent).

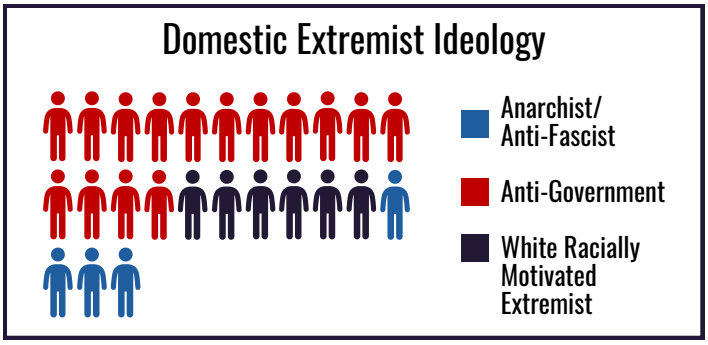
Domestic Extremist Platform Breakdown



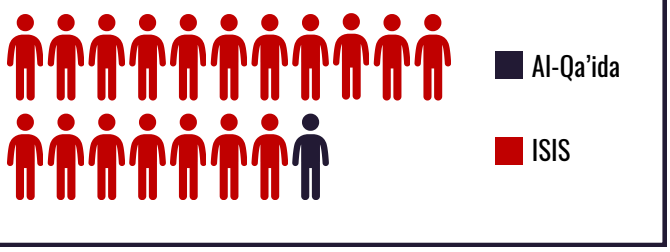
HVE Platform Breakdown



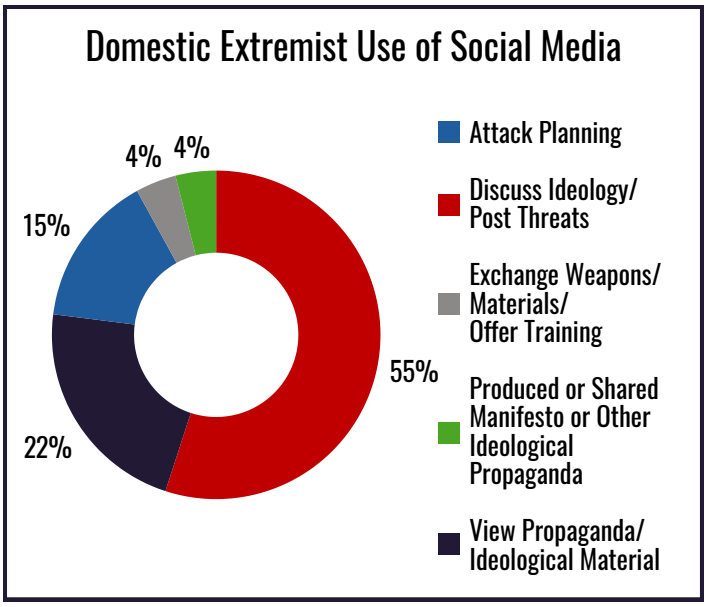
Domestic Extremist Ideology

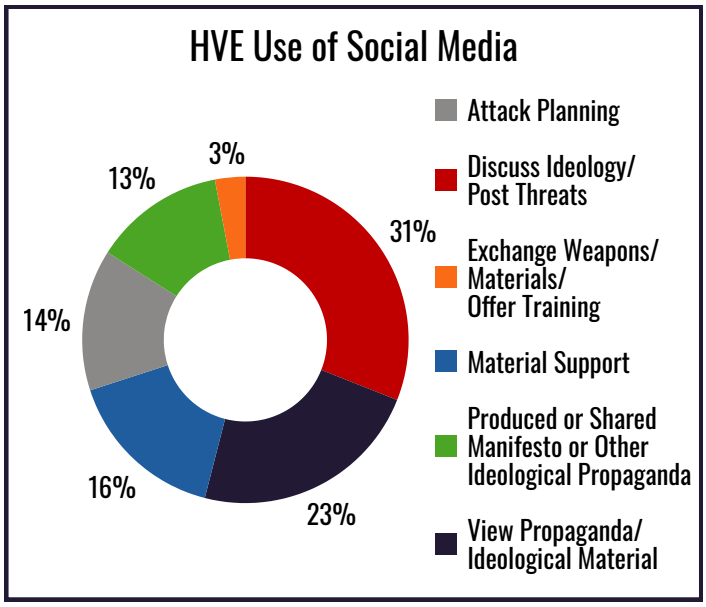


HVE Group Influence

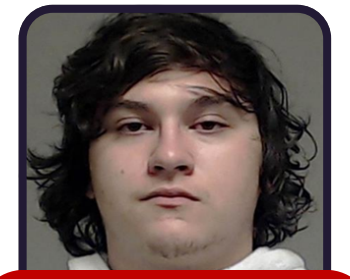


Domestic and Homegrown Violent Extremist Use of Social Media





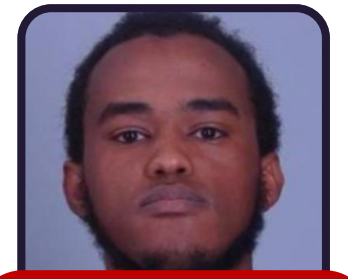
SEP 2025



Operated online under the monikers "Frank Hoenniker," "#Impeachment," and "Hankiebob"

Authorities arrested Joshua Jahn, of Texas, for shooting toward a Dallas U.S. Immigration and Customs Enforcement (ICE) facility, killing two detainees and injuring another. Prior to the attack, Jahn allegedly used social media platforms, such as Facebook, X, Reddit, 4chan, and Discord to mock political figures, comment on immigration, and share anti-fascist and communist imagery. According to authorities, Jahn inscribed "ANTI-ICE" on a bullet and left notes detailing his desire to ambush and terrorize ICE agents. Jahn allegedly practiced shooting in-person and used ICE tracking apps to download information about local facilities in preparation for the attack.

FEB 2025



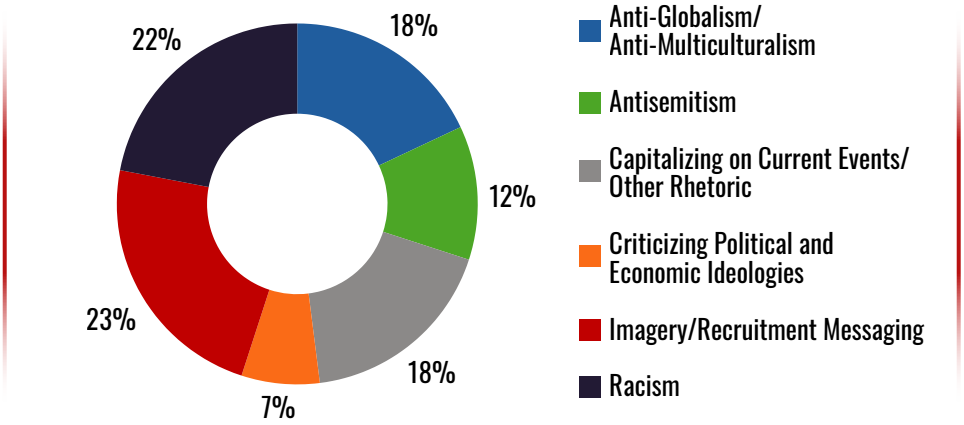
Operated online under the usernames "Qays Man," "expand_my _state1," and "jundullah032"

Authorities arrested Abdisatar Ahmed Hassan, of Minnesota, after he attempted to travel and allegedly join ISIS in Somalia. According to authorities, Hassan shared his support for ISIS on Facebook and TikTok by posting propaganda and praise for prior attacks. In one post, he shared a video of himself driving around with an ISIS flag. On Facebook, Hassan allegedly communicated with the Manjaniq Media Center, a media organization affiliated with ISIS. Hassan also allegedly used Telegram to consume propaganda and share links to documents detailing sniper skills and other training materials.

Extremist Propaganda Discovered in New Jersey

Since 2019, domestic extremists have vandalized publicly accessible locations with propaganda using a variety of signs, promoted extremist beliefs that disparage those with opposing views, and used images and symbols to promote their ideology and motivate supporters to engage in physical activities. To better understand the tactics and messaging extremists use to distribute their propaganda, the New Jersey Office of Homeland Security and Preparedness reviewed and analyzed approximately 1,200 pieces of material belonging to a variety of groups, either online or in-person.

2019-2025 Propaganda Themes



Most of the propaganda included an assortment of signs, stickers, posters, fliers, and spray-painted graffiti in varying shapes and sizes to draw attention from pedestrians. Bumper stickers with minimal wording, imagery, and slogans were the most common form of propaganda. These materials have been displayed on traffic signs, telephone poles, electric boxes, and various locations, including in and around commercial parking lots, gas stations, and other public venues. Some groups participated and displayed their propaganda during in-person protest activities, banner drops, hiking and training events, and recruitment efforts.

Reoccurring themes consisted of antisemitism, nationalism, anti-immigrant, and racist messaging that targeted and intimidated ethnic minorities and religious groups. Other pieces of propaganda included dismissing communism, socialism, and supporting anti-fascist ideologies. Certain messaging also included praise for mass shooters, exploiting murder victims to blame and disparage a specific ethnicity, and seeking justice for individuals who are allegedly associated with extremist groups. There were no references or threatening language towards New Jersey legislators or messages encouraging supporters to target or attack a town, city, county, community, or any specified individuals.

Several groups have used similar symbols and imagery to distinguish their propaganda from other extremists. One group has relied on similar aesthetics using a red and blue color scheme, bald eagles, and stars and stripes to claim they are patriots defending the country from minorities. Another common symbol from a separate group used an image of a gladiator to illustrate their strength and desire to fight their perceived enemies. Individuals who documented their in-person activity were usually disguised in masks to conceal their identity to avoid detection.

Targeted Violence Threatens Religious Communities

Various extremists who adhere to a blend of violent ideologies and conspiracy theories will plot and attack religious communities, houses of worship, and faith-based institutions. In 2025, individuals in New Jersey communicated explicit or implied threats to intimidate faith-based communities compared to national trends that have involved extremists independently plotting and successfully conducting non-fatal and fatal attacks.

OCT 2025

Authorities arrested Louis Geri, of Vineland (Cumberland County), outside the Cathedral of Saint Matthew the Apostle in Washington, D.C. Geri allegedly assembled a tent on the top of the stairs leading to the cathedral and refused to leave. Law enforcement observed multiple suspicious items inside the tent, including possible fireworks, bottle rockets, and Molotov cocktails.

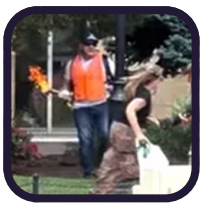
SEP 2025

Thomas Sanford rammed his pickup truck into a Church of Jesus Christ of Latter-Day Saints in Grand Blanc, Michigan. According to authorities, after exiting his vehicle, he shot and killed four people, injured eight others, and set fire to the building. Responding officers killed Sanford during a shootout.

JUL 2025

A 16-year-old from Lombard, Illinois, was arrested for plotting to attack a suburban Islamic center. Officials said he conducted preoperational planning by entering the center and recording religious services to assist him in conducting an attack using an explosive device.

JUN 2025



Mohamed Soliman allegedly used a “makeshift flamethrower,” as well as Molotov cocktails, to attack a “Run for Their Lives” event in Boulder, Colorado, killing one and injuring eight. The event sought to bring awareness to Israeli hostages in Gaza.

Nationwide Incidents Drive Rise in NJ Threat Reporting

From January to December, the New Jersey Office of Homeland Security and Preparedness received over 150 reports impacting religious communities, facilities, and schools. Thirty percent of threats were delivered in person, but a notable amount were made verbally and on social media. The months with the most reported incidents were October and December.

- The top five counties with the highest number of reports were Bergen, Camden, Essex, Middlesex, and Union.
- About 17 percent of reported incidents were ideologically motivated or had a nexus to a foreign extremist ideology.
- More than half of the incident types were Expressed or Implied Threats. The next most common incident types were Sabotage/Tampering/Vandalism and Recruiting/Radicalizing.

National Incidents Inspire Government-Related Threats in New Jersey

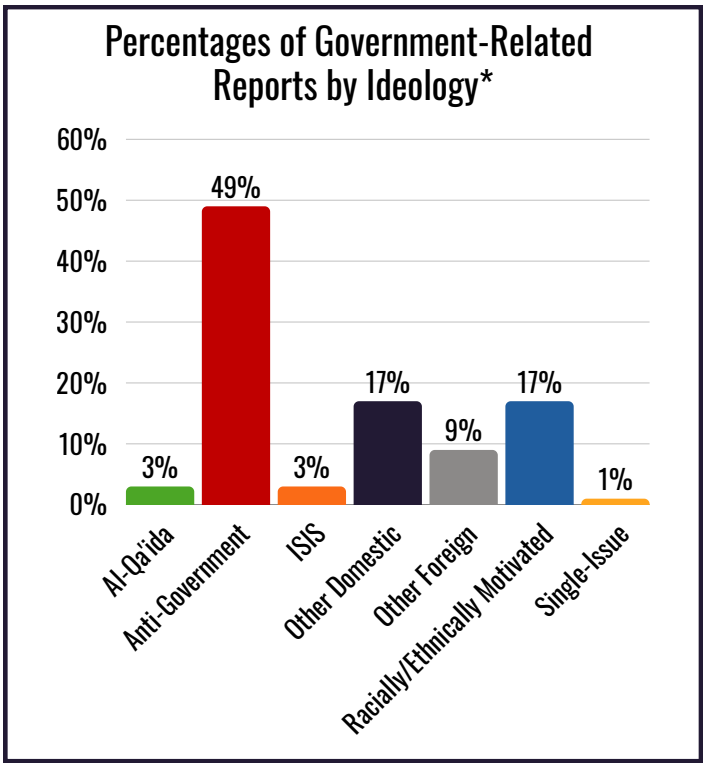
Accompanying a national increase in high-visibility attacks targeting elected officials, New Jersey has seen an uptick in reporting within the Government Services and Facilities sector, indicating national events may be inspiring individuals to make similar plots and threats in the state. In 2025, extremists who subscribed to a variety of ideologies targeted government personnel, elected officials, and other figures symbolic of government. The sector is also inclusive of physical buildings owned or leased by any level of government.

NOV 2025

Authorities arrested Keith Lisa for allegedly attempting to confront former U.S. Attorney for the District of New Jersey Alina Habba. According to authorities, Lisa initially arrived at the federal building with a baseball bat, was denied entry, and later returned without a weapon. After gaining access, he allegedly vandalized Habba's office.

APR 2025

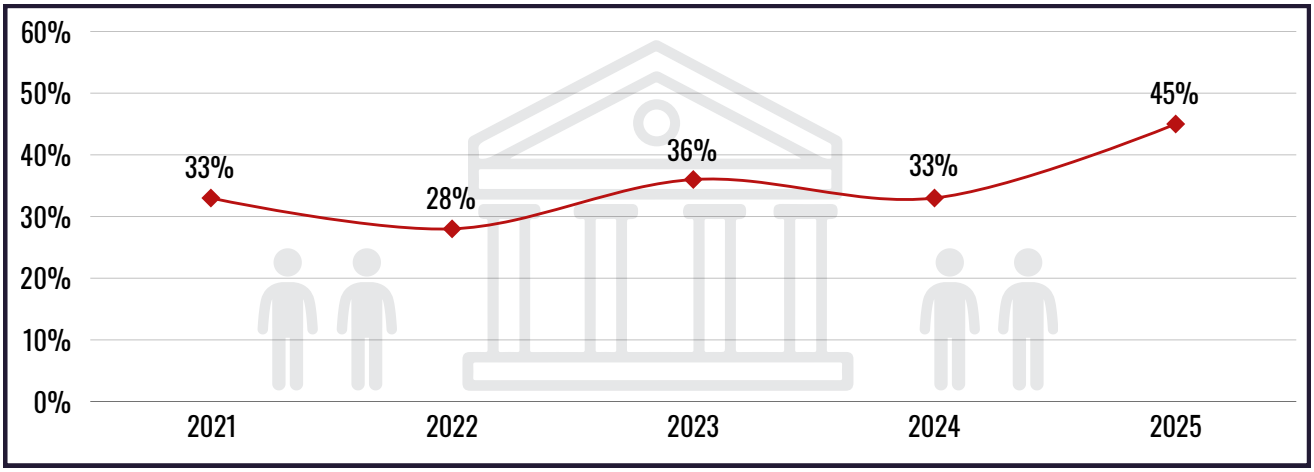
Esther Salas, a U.S. District Court Judge for New Jersey, and other judges, received pizza deliveries to their homes as a threat and intimidation tactic. The name of Salas's son, who was murdered in 2020 by a gunman posing as a delivery man, was attached to the order. This tactic was done on a national stage as many judges around the U.S. received the pizza delivery.



*Percentages rounded to the nearest whole number; totals may not equal 100%

Government Personnel Related Reports

Nationally, there has been an increase in the targeting of elected officials and other government personnel. A five-year review of government-related reports the New Jersey Office of Homeland Security and Preparedness received showed a similar pattern within the state, with an uptick in reports involving the targeting of government personnel.



National Incidents Targeting the Government Services and Facilities Sector

In a five-year review of national incidents targeting the Government Services and Facilities sector, there were a total of 30 attacks, 17 threats, and 15 plots, with 14 of these incidents occurring in 2025. From 2021 to 2025, most threat actors (23) embraced anti-government ideologies, followed by anarchist/anti-fascist ideology (14). Individuals used small arms in most incidents (19), and relied on vandalism (12), improvised explosive devices (IED) (11), and arson (9) as the next most common methods.

JUN 2025

Vance Boelter allegedly impersonated a law enforcement officer and targeted several Minnesota legislators and their spouses in their homes in separate attacks, killing two. According to authorities, Boelter wore a police-style tactical vest, badge, and a silicone mask and allegedly conducted preoperational surveillance of the residences, identifying addresses and occupants.

APR 2025

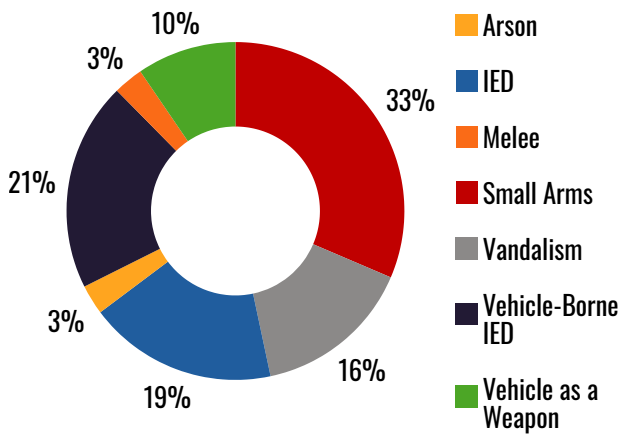
Cody Balmer, of Pennsylvania, allegedly threw an improvised incendiary device (IID) into Pennsylvania Governor Joshua Shapiro's residence. Balmer reportedly disapproved of Gov. Shapiro's stance on the Israel-HAMAS conflict and told 911 dispatchers that he "will not take part in his plans for what he wants to do to the Palestinian people." The attack took place on the first night of Passover and occurred while residents were sleeping. Balmer allegedly climbed the perimeter fence, broke two windows, and proceeded into the residence, throwing two IIDs before fleeing.

FEB 2025

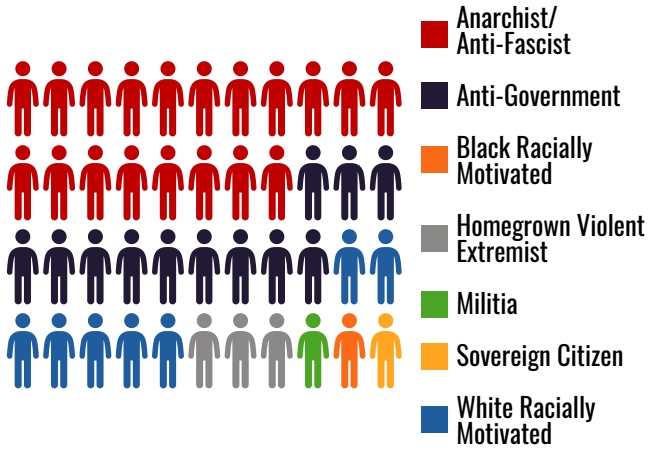
Authorities arrested Nikita Casap, of Wisconsin, for allegedly killing his parents as part of his plot to assassinate President Donald Trump and overthrow the government. According to authorities, materials recovered from his residence praised Adolf Hitler and indicated that Casap identified with the neo-Nazi group Order of the Nine Angles. One month before the murders, Casap allegedly communicated with an unidentified individual believed to be in Russia and discussed his plan to assassinate President Trump and then flee to Ukraine.

Review of 2021-2025 Incidents

Methods Used Against This Sector



Extremist Ideology



Threat Landscape Shift: Healthcare and Public Health Sector (2020-2025)

Healthcare-related reports in New Jersey have more than doubled from 2020 to 2025. While the initial increase in this reporting was likely in response to the COVID-19 pandemic, reporting in subsequent years has surpassed the COVID-19-related spike despite the pandemic waning, indicating a possible shift from ideologically motivated threats to grievance-based threats. In 2025, there were several ideologically driven national attacks targeting the Healthcare and Public Health sector. Concurrently, New Jersey has seen an increase in healthcare-related reports, suggesting that threat actors, though not ideologically motivated themselves, may be motivated by national events.

Polarization early in the COVID-19 pandemic drove an initial increase in reports involving the Healthcare and Public Health sector in 2020. Although polarization diminished as restrictions lifted in 2021, threats to the sector persisted, suggesting the pandemic elevated the sector's profile among threat actors by increasing public attention and media scrutiny. This heighted visibility made the sector more attractive to threat actors in the subsequent years.

Sector Overview

The Healthcare and Public Health Sector protects all sectors of the economy from hazards such as terrorism, infectious disease outbreaks, and natural disasters. New Jersey has one of the largest concentrations of pharmaceutical and biotechnology companies in the U.S.

Reports from 2025 show a pattern of threats made by unsatisfied patients targeting healthcare facilities, which deviates from previous years' reporting of individuals targeting the sector due to grievances related to public health policy. These 2025 threats, most frequently articulated as shooting or bomb threats, were delivered in-person, online, and by telephone.

The majority of healthcare-related reports from 2020 to 2025 were expressed or implied threats with the intent of committing harm toward individuals or damaging a facility, infrastructure, or secured site. These threats often cite personal grievances such as perceived inadequate care or denial of services as an apparent motivation.

High-Profile Incident Drives Rise in NJ Threat Reporting

In December 2024, Luigi Mangione allegedly shot and killed the UnitedHealthcare CEO in New York City. Mangione was allegedly motivated by personal frustrations and anger with the American healthcare and insurance industry. Since then, New Jersey has received an influx of reports citing this shooting as a justification for threatening violence. In a May 2025 report, an online threat against a New Jersey-based pharmaceutical company stated that the individual "dreamed every day" of "Luigi Mangioning" its CEO. Similar threats have been made against other New Jersey-based executives outside of the healthcare sector.

Assessing FTO and Domestic Extremist UAS Usage

Domestic extremists, homegrown violent extremists (HVEs), and foreign terrorist organizations (FTOs) are demonstrating growing interest in using unmanned aircraft systems (UAS) for attack planning, delivery of explosives, and preoperational surveillance. During the summer of 2026, New Jersey and multiple other states will be hosting a series of high-profile, high-attendance events. These events may attract the attention of extremists who could incorporate drones into planning or activities aimed at disrupting or threatening public safety.

In 2025, the U.S. Department of Homeland Security (DHS) stated in its annual Homeland Threat Assessment that HVEs and other ideologically motivated extremists are considering, "using UAS to conduct intelligence collection, to drop explosives and other items on U.S. critical infrastructure for disruption purposes, and to endanger takeoffs and landings at airports."

NOV 2024

Authorities arrested Skyler Philippi, of Tennessee, for plotting to attack an interstate electrical substation with a drone. Philippi shared his desire with a confidential human source, stating that attacking a large substation would "shock the system," causing other electric substations to malfunction. He wrote a manifesto expressing his desire to attack "high tax cities or industrial areas," and allegedly revealed a prior association with two white racially motivated extremist (WRME) groups.

OCT 2024

Authorities arrested HVE Marvin Jalo in Arizona for plotting an ISIS-inspired attack in which he planned to detonate an improvised explosive device (IED) at the Phoenix Pride Festival. Between November 2023 and May 2024, Jalo discussed the supplies for making an IED in chat rooms and had the supplies shipped to him. He then posted videos of himself making explosives. On Telegram, Jalo discussed using a drone to deliver his explosives in Phoenix and attacking other targets, including New York City.

MAR 2019

Brenton Tarrant, a WRME, attacked two mosques in Christchurch, New Zealand, killing 51 individuals. He used a UAS from a nearby park to conduct preoperational planning. Tarrant flew a hobby drone over the Al Noor Mosque roughly two months before the attacks, studying the entry and exit points and the mosque's grounds.

How FTOs Utilize UAS

FTOs, such as ISIS and al-Qa'ida, use UAS for surveillance, reconnaissance, and media production, and depending on capability, have conducted limited strikes on physical locations. These sites are primarily in the Middle East and Africa where the groups and affiliates operate. Despite FTOs regional focus, the groups routinely advocate for their supporters to target Western nations and conduct mass casualty incidents, including in the U.S., and have historically referenced and encouraged UAS as a method of attack.

Threats to High Profile Events

Major events and mass gatherings, such as the upcoming FIFA World Cup 2026 and Sail4th 250, continue to face a heightened threat environment as evidenced by recent attacks, disrupted plots, and propaganda releases from a variety of violent extremist movements. These high-profile events, which will draw large crowds from around the world, can also be potential targets of disruptive or otherwise criminal actions, including physical assault, harassment, intimidation, vandalism, and property damage.

The New Jersey Regional Operations & Intelligence Center (NJ ROIC) currently has no information indicating any specific or credible threats to these or other upcoming large-scale events in New Jersey, including, but not limited to, the FIFA World Cup 2026 and Sail4th 250. The NJ ROIC remains aware of the potential risk posed by lone offenders motivated by personal grievances, as well as broader calls for violence issued by extremist organizations. These events are expected to have both foreign and domestic high-level government officials in attendance, making them attractive targets for violent extremists hoping to achieve global notoriety, either at the events or during the movement of the officials.

The NJ ROIC assesses that a wide range of malicious actors will continue to attempt to inspire supporters, both through online calls for violence and extremist messaging to initiate attacks. ISIS continues to publish propaganda calling for lone-offender attacks in the U.S. In 2024, ISIS released a series of propaganda posters inciting attacks against major sporting event venues. While this campaign appeared to be a more general threat to major sporting events, it established a targeting focus on international soccer, indicating similar efforts may follow around the time of the FIFA World Cup 2026. In September 2025, the U.S. National Counterterrorism Center warned that al-Qa'ida and its Yemen-based affiliate, al-Qa'ida in the Arabian Peninsula, had issued calls to attack Western assets and urged its followers to target high-profile public venues, such as sports and music events.

Previous attacks and plots against special events and other soft targets in the U.S. and Europe underscore the potential for extremists and violent actors to encourage and inspire attacks that exploit security vulnerabilities at mass events. Recent tactics highlight the vulnerabilities of these venues with actors utilizing vehicle-ramming, improvised explosive devices, improvised incendiary devices, suicide attacks, and readily available methods, such as edged weapons, firearms, blunt objects, chemical splashes and spray attacks, and arson.

Notable Events in 2025 Targeting Mass Gatherings

December: ISIS planned to carry out attacks in Turkey, focusing on non-Muslims during Christmas and New Year's events before Turkish police disrupted the plot and detained 115 suspected members of the militant group.

December: Authorities disrupted separate mass-casualty plots in Southern California and North Carolina that were planned for New Year's Eve celebrations. The California suspects were allegedly part of an anti-government group and were found with bomb-making materials.

December: Two gunmen allegedly opened fire at a Hanukkah celebration in Bondi Beach, Australia, killing 15 and leaving dozens wounded. According to authorities, both had pledged allegiance to ISIS before the attack.

December: German authorities arrested five men suspected of planning an "Islamist-motivated" vehicle ramming attack at a Christmas market.

July: An individual allegedly drove his vehicle with intent into a crowd outside of a nightclub in Los Angeles, injuring 30 individuals. The driver had been kicked out of the club before the attack.

June: One hundred forty-five individuals were jabbed with syringes during the Fête de la Musique, a music festival in France. Victims reported feeling hot flushes, dizziness, loss of consciousness, and visible injection marks on their skin.

January: An individual carried out a vehicle ramming attack on New Year's Day in New Orleans, killing 14. The individual allegedly had an ISIS flag on his vehicle during the attack.

COUNTERINTELLIGENCE

Counterintelligence Awareness: Securing the Garden State from Foreign Threats

New Jersey's strategic location, dense network of critical infrastructure, and significant concentration of sensitive technological industries, financial institutions, and academic research centers make it a prime target for foreign intelligence entities (FIEs) and nation-state actors. Foreign adversaries, particularly the People's Republic of China (PRC), Russia, and Iran, routinely engage in intelligence-gathering activities aimed at undermining U.S. economic and national security. It is incumbent upon all New Jersey residents and businesses to ensure the state's security and economic stability.

The Nature of the Threat

Counterintelligence involves efforts to identify, counter and protect against espionage, sabotage, or other intelligence activities conducted by or at the behest of foreign governments. In New Jersey, these threats primarily manifest across three domains: economic espionage, cyber operations, and foreign malign influence.

What Are Foreign Intelligence Entities?

Foreign intelligence entities are known or suspected foreign state or non-state organizations or persons that conduct intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. The term includes foreign intelligence and security services and international terrorists.

Economic Espionage and Intellectual Property Theft

FIEs seek to steal sensitive proprietary information, research and development data, and emerging technologies. Theft of intellectual property allows foreign competitors to bypass years of costly research, significantly weakening the U.S. economic and competitive edge.

Adversaries often recruit individuals with access through deceptive means, such as academic partnerships, corporate joint ventures, or financial incentives. They exploit the open nature of American society and use non-traditional collectors, including students, researchers, and seemingly legitimate business people.

Foreign actors rely heavily on trusted insiders as attack vectors. The New Jersey Office of Homeland Security and Preparedness defines counterintelligence insider threats as individuals with authorized access who exploit their position to steal information, either wittingly or unwittingly. This can include employees, contractors, or even business partners at firms across the Garden State.

Cyber Operations and Critical Infrastructure Sabotage

Groups such as the PRC's Volt Typhoon have been cited for pre-positioning themselves within the networks of U.S.-based critical infrastructure. This access allows them to monitor systems and potentially disrupt or disable services in a future conflict. A cyberattack on an energy grid or water treatment facility in New Jersey could immediately impact public health and safety.

Ransomware attacks against New Jersey public- and private-sector organizations are costly and operationally debilitating, causing significant financial damage and service downtime. While often financially motivated, the sophisticated cybercriminal groups behind ransomware attacks often have affiliation with, or tacit support from foreign governments, thereby complicating threat attribution.

Adversaries frequently use sophisticated phishing and other social engineering schemes to steal network credentials, which remain one of the most prevalent initial access vectors into victim networks. This can apply equally from a large corporation to a local government office.

Foreign Malign Influence

Foreign actors have conducted transnational repression operations in New Jersey to harass, surveil, and coerce expatriates to return to their home country to face criminal prosecution. Adversaries continue to use the cover of academic organizations to target and recruit individuals in New Jersey who have access to sensitive information. This involves identifying university professors, researchers, and others with access to sensitive technologies or equipment to gather intelligence and secure dual-use technologies, leveraging the state's research and defense sectors.

Foreign governments use sophisticated online disinformation and misinformation campaigns to sow discord, amplify social divisions, widen political divides, and undermine confidence in democratic processes and institutions among the New Jersey population. These campaigns utilize fictitious social media accounts, fabricated headlines, and artificial intelligence (AI)-generated content to spread propaganda (for example, election interference efforts or narrative shaping during conflicts such as the current war between Russia and Ukraine).

Operation Fox Hunt

On April 16, a federal court sentenced Michael McMahon, of Mahwah (Bergen County), to 18 months in prison for acting as an illegal agent of the PRC, interstate stalking, and conspiracy. McMahon, a retired New York City Police Department officer, participated in the PRC's international repatriation effort known as "Operation Fox Hunt," which targeted a U.S. resident and his family. Between 2016 and 2019, McMahon and co-conspirators threatened, harassed, surveilled, and intimidated the family to force their return to the PRC to face purported corruption charges, as part of the PRC's broader "Operation Sky Net." A federal jury convicted McMahon and co-defendant Zhu Yong in June 2023; Zhu and a third defendant, Congying Zheng, were sentenced earlier in January to 24 months and 16 months, respectively.

The Role of Counterintelligence

Counterintelligence awareness shares the responsibility of defense with the community at large. When New Jersey residents and businesses are vigilant, they become the "first line of defense," creating a more difficult operating environment for foreign actors.

Responsibility of Residents

Residents are often unwittingly targeted as access points to larger organizations or as part of malign influence campaigns. Foreign governments utilize social engineering to manipulate individuals into divulging confidential information, compromising both personal and professional data. This includes sophisticated phishing emails, texts, and calls. Residents should be suspicious of unsolicited or unusual requests for information.

Russia and Iran are known for leveraging disinformation and misinformation campaigns using social media platforms and state-controlled media outlets. These campaigns seek to sow discord, erode trust in government institutions, and influence public opinion, particularly around elections or international crises. Residents must critically evaluate the sources of information they consume and share, guarding against manipulation that can incite real-world harm. Visit njohsp.gov/threat-landscape/disinformation for more information on how to recognize disinformation.

The Importance for Businesses

For New Jersey businesses (particularly those in biotechnology and pharmaceutical research, emerging technologies, defense and security, or finance), counterintelligence awareness is vital to the company's long-term success and viability.

Businesses must implement robust counterintelligence programs to protect their intellectual property, trade secrets, and proprietary data. Simple measures like mandatory multifactor authentication (MFA), regular employee counterintelligence training, and clearly defined policies for reporting suspicious activity and handling sensitive information are essential.

Businesses should exercise caution and conduct due diligence when engaging with foreign entities, particularly for sensitive research and development projects or supply chain components that originate from high-risk countries. Rigorous vetting and continuous monitoring of key personnel, such as those with access to sensitive information, are crucial to mitigating insider threats.

New Jersey Case Highlights

AUG 2025

A federal court sentenced Vadim Yermolenko, of Upper Saddle River (Bergen County), and dual U.S./Russian national, to 30 months in prison for his role in a transnational arms dealing and money laundering network. This network sought to acquire ammunition and highly sensitive, export-controlled dual-use electronics—some usable in nuclear and hypersonic weapons and quantum computing—for Russian military and intelligence services. Yermolenko was affiliated with the Moscow-based procurement companies Serniya Engineering and Sertal LLC. These companies used a vast global network of shell companies and bank accounts, including in the U.S., to conceal the Russian government's involvement and the true Russian end-users of the U.S.-origin equipment.

JUN 2025

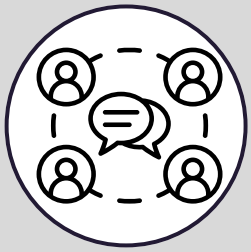
The U.S. Attorney's Office for the District of Massachusetts, National Security Division, announced the indictment of New Jersey resident Zhenxing "Danny" Wang, on five counts. The indictment details a multi-year fraud scheme by Wang and co-conspirators that generated over $5 million by securing remote information technology work with U.S. companies. In addition to Wang, authorities also charged Chinese nationals Jing Bin Huang, Baoyu Zhou, Tong Yuze, Yongzhe Xu, Ziyou Yuan, and Zhenbang Zhou, and Taiwanese nationals Mengting Liu and Enchia Liu. A second New Jersey resident, Kejia "Tony" Wang, was charged separately and has agreed to plead guilty for his role in the scheme.



CYBERSECURITY

New Jersey Cybersecurity and Communications Integrations 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 (NJOHSP). The NJCCIC works to make New Jersey more resilient to cyberattacks by promoting statewide awareness of cyber threats and widespread adoption of best practices. The NJCCIC provides 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, which are the strongest defenses against cyberattacks. Visit cyber.nj.gov/connect/njccic-membership to join today at no cost 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.

Nation-state adversaries represent the most sophisticated and persistent cyber threats facing New Jersey and the nation. These actors possess significant resources, advanced capabilities, and strategic patience to conduct long-term campaigns targeting critical infrastructure, intellectual property, and sensitive information to advance their respective military, political, and economic agendas. The New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) assesses that State-sponsored cyber activity is expected to remain a top threat in 2026 and beyond.

The People's Republic of China (PRC)

The PRC poses the greatest long-term threat to New Jersey and U.S. national security in cyberspace. PRC-linked state-sponsored cyber actors continue to conduct sustained and strategically aligned cyber operations against U.S. critical infrastructure, with the assessed objective of pre-positioning for disruptive or destructive attacks during a future geopolitical crisis. Advanced persistent threat (APT) groups such as Volt Typhoon, Salt Typhoon, and Silk Typhoon have demonstrated the capability to gain and maintain long-term access to communications, energy, water and wastewater, and transportation systems by exploiting compromised credentials, unpatched edge devices, and trusted third-party access. Unlike traditional espionage-focused activity, these operations are designed to enable rapid activation and cascading service disruption, threatening emergency response, military mobilization, economic stability, and public safety. The NJCCIC assesses that this activity represents an ongoing enduring risk that will intensify as global tensions increase. Chinese state-sponsored cyber operations are expected to increase with escalating geopolitical tensions. The NJCCIC anticipates that these threats will continue to evolve in scale and sophistication. Critical infrastructure organizations should view this threat activity as a persistent risk.

Volt Typhoon: This PRC-linked threat group has maintained persistent access to U.S. water, energy, transportation, and communications systems for over five years. Volt Typhoon's primary objective is to gain and maintain covert, long-term access to U.S. and allied critical infrastructure networks to enable potential disruption or sabotage during a future geopolitical crisis or armed conflict, such as an invasion of Taiwan. The threat actor group gains initial access to target networks by exploiting unpatched or end-of-life vulnerabilities in internet-facing devices and utilizing compromised credentials. Once inside its targets' networks, Volt Typhoon uses "living off the land" (LotL) techniques, which involve using built-in Windows system administration tools, such as PowerShell, netstat, and RDP, to maintain persistent access while evading detection.

Salt Typhoon: This espionage-focused operation attributed to the PRC's Ministry of State Security (MSS) has infiltrated global telecommunications, government, and critical infrastructure networks, including at least nine telecommunications carriers in the U.S. The primary goal of Salt Typhoon is long-term intelligence gathering and to gain a persistent, pre-positioned ability to disrupt essential services during a future geopolitical crisis. Like its Volt Typhoon counterpart, Salt Typhoon typically gains initial access into target networks by exploiting unpatched vulnerable edge devices or using compromised credentials and then maintaining persistence inside victim networks using LotL techniques. Salt Typhoon operations date back to 2019 and are still active today.

Silk Typhoon: This espionage-focused PRC APT is attributed to the MSS. It is also known as HAFNIUM, which previously compromised Microsoft Exchange email servers worldwide using four zero-day vulnerabilities in 2021. More recently, Silk Typhoon has shifted to targeting information technology supply chains, including remote management tools, cloud applications, and privileged access management platforms to compromise downstream customer environments. In January 2025, the U.S. Department of Justice identified Silk Typhoon as the organization that infiltrated the networks of the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) and the Committee on Foreign Investment in the United States (CIFUS) by exploiting vulnerabilities in Treasury's cloud-based vendor's identity management product. In early 2025, the PRC-linked threat group Silk Typhoon exploited a zero-day vulnerability in Commvault's Metallic SaaS backup platform to access application secrets belonging to a subset of the company's North American customers. Microsoft Threat Intelligence first identified the intrusion and notified Commvault in late February. CrowdStrike later corroborated the attribution in an August 2025 report.

UNC5221: In October 2025, the PRC APT group that Google/Mandiant identifies as UNC5221 was discovered to have maintained unauthorized access to F5 Networks' production and development environment for at least 12 months, stealing BIG-IP source code and undisclosed vulnerability data. F5 is a major technology vendor that sells application security and data delivery products to over 23,000 enterprise-level customers worldwide. This breach and UNC5221's access to F5's source code and vulnerability data creates risk of future cyberattacks against F5 customers.

Foreign-Malign Influence and Transnational Repression Cyber Operations: Beyond traditional cyber espionage and critical infrastructure prepositioning, the PRC also leverages its cyber capabilities to conduct foreign malign influence and transnational repression operations aimed at shaping narratives, silencing critics, and coercing members of diaspora communities. These activities frequently blend cyber operations with information operations, harassment, and intimidation.

Leading up to the 2024 U.S. presidential election, PRC-sponsored actors conducted foreign malign influence operations known as Spamoflage (aka Dragonbridge) using fake social media accounts to impersonate American voters and sow social division. In parallel, PRC actors have supported transnational repression efforts by using cyber means to surveil, harass, and threaten overseas dissidents, including through the compromise of personal accounts, doxing, and online coercion tied to broader initiatives such as Operation Fox Hunt, which began in 2014 and seeks to pressure individuals abroad to return to the PRC. In March 2025, Quanzhong An, of New York, was sentenced to 20 months in prison for acting as an illegal agent of the PRC and a leader in the Operation Foxhunt operation. The NJCCIC assesses that like its other cyber operations that support its strategic initiatives, the PRC's state-sponsored operators will continue to conduct foreign malign influence and transnational repression campaigns.

The above examples are just several of the PRC's state-sponsored cyber operations. The NJCCIC assesses that in 2026 and beyond, these operations will continue to evolve in scale and sophistication. For more information, readers are encouraged review the NJCCIC's Threat Analysis Report: China-Linked Cyber Operations Targeting U.S. Critical Infrastructure.

The Russian Federation

Russia's intelligence services, including the Federal Security Service (FSB), the Main Directorate of the General Staff of the Armed Forces (GRU), and the Foreign Intelligence Service (SVR) conduct extensive cyber operations targeting government, military, diplomatic, and private-sector organizations worldwide in support of Russia's foreign policy and military objectives. Russian state-sponsored cyber actors are highly capable, developing custom malware, exploiting zero-day vulnerabilities, and increasingly leveraging LotL techniques to evade detection. Throughout 2025, Russia's cyber operations remained largely focused on the ongoing war in Ukraine and spying on NATO countries, but they also broadened to strike at global targets, frequently under the guise of hacktivism.

GRU APTs: Over the past decade, the GRU-linked Sandworm APT has repeatedly shown its capability to disrupt critical infrastructure. In 2015 and 2016, Sandworm was responsible for hacking into and taking down parts of Ukraine's power grid. In 2017, Sandworm launched the NotPetya malware, which became the most damaging cyberattack in history. This attack caused over $10 billion in global damage, including an estimated $1.4 billion impact in New Jersey (hitting Merck and the Port of Newark). In 2019, the U.S. Department of Justice in Pittsburgh indicted six members of the GRU for their roles in the NotPetya attack and also cited the GRU's role in the Ukraine power grid hacks. In May 2025, the U.S. Department of Homeland Security (DHS), Cybersecurity Infrastructure and Security Agency (CISA), and allied agencies warned that GRU Unit 26165 (APT28/Fancy Bear) was actively targeting Western logistics entities and technology companies supporting Ukraine aid delivery, seeking intelligence on foreign assistance shipments. The GRU has also expanded its use of proxy hacktivist groups, including KillNet, NoName (057) 16, Cyber Army of Russia Reborn (CARR), and Z-Pentest, to conduct disruptive attacks against U.S. and European critical infrastructure while maintaining plausible deniability. In 2024, the NJCCIC identified CARR infiltrations into the Supervisory Control and Data Acquisition (SCADA) infrastructure of four New Jersey municipal water systems. In April 2025, the hacktivist group Z-Pentest compromised the control systems of a dam in Norway and remotely opened a sluice gate, causing water release for four hours. NoName (057)16 is the most prolific of the hacktivist groups carrying out distributed denial-of-service (DDoS) attacks against networks in Ukraine and in countries allied with Ukraine. In December 2025, the U.S. Department of Justice announced two indictments in California charging Ukrainian national Victoria Dubranova for her role in conducting cyberattacks and computer intrusions against critical infrastructure in support of Russia's geopolitical interests. The indictment cited Dubranova's role within CARR and NoName (057) 16, and linked these groups activities to the GRU.

SVR APTs: Midnight Blizzard (aka APT29/Cozy Bear) is a Russian cyber espionage group that has been formally linked to Russia's SVR by CISA, the NSA, and the FBI. The SVR primarily focuses on espionage operations and intelligence collection targeting government agencies, think tanks, and technology companies in Western countries. U.S. intelligence agencies and several cybersecurity companies have attributed the following cyberattacks to the SVR. In 2025, Midnight Blizzard targeted European diplomats with sophisticated phishing campaigns using wine-tasting event invitations and eventually gaining access to their targets' systems and accounts. In late 2023 and 2024, Midnight Blizzard compromised Microsoft's corporate email system where they 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 Microsoft's customers' emails, including that of federal and State government organizations. The SVR was also responsible for the 2020 SolarWinds supply chain compromise, in which Russian cyber actors inserted malicious code into software updates to infiltrate the networks of U.S. government agencies and thousands of private sector organizations worldwide. The NJCCIC assesses that Russia represents one of the most formidable and aggressive nation-state cyber threats capable of conducting destructive attacks against critical infrastructure, exploiting zero-day vulnerabilities, and leveraging proxy hacktivist groups to maintain plausible deniability while pursuing strategic objectives.

Islamic Republic of Iran

Iran's cyber program continued to mature in 2025, as Iranian groups conducted aggressive operations in both the Middle East and abroad. Iranian state-sponsored hackers, such as MuddyWater, Charming Kitten, and CyberAv3ngers, focus on spying on adversaries (including Israel, Gulf states, and the U.S.) and sometimes on retaliatory sabotage. In 2025, an escalating factor was the conflict between Israel and HAMAS during which Iranian cyber units and proxy hackers ramped up attacks on Israeli organizations and any entities perceived as supporting Israel. Despite the October ceasefire, these Iranian Islamic Revolutionary Guard Corps (IRGC)-aligned APTs and their hacktivist proxies continue to carry out attacks on Israeli networks and those of its allies and supporters. Over the past year, more than 170 hacktivist groups supporting HAMAS and Iran have carried out cyberattacks against Israeli networks and those they deemed to be supporters of Israel.

CyberAv3ngers: Affiliated with Iran's IRGC, this APT group continued targeting Israeli-linked water systems and other critical infrastructure with its custom IOCONTROL malware designed to target Programmable Logic Controllers (PLCs), Human Machine Interfaces (HMIs) and SCADA systems. In June 2025, the U.S. State Department issued sanctions against the leaders of the IRGC Cyber-Electronic Command and a $10 million reward for information on individuals associated with CyberAv3ngers, citing ongoing attacks against U.S. critical infrastructure. With heightened tensions, including those related to U.S. sanctions and Iran's nuclear ambitions, Iran may seek to retaliate via cyber means in 2026, potentially aiming at soft targets such as local government networks, financial services, and entities perceived as opponents of Iran or allies of Israel.

Democratic People's Republic of Korea (DPRK)

North Korea's cyber operations serve as a critical revenue generation mechanism for the regime, with cryptocurrency theft funding weapons programs and circumventing international sanctions. North Korean intelligence bureaus, such as the Reconnaissance General Bureau (RGB), conducts the nation's cyber operations. The Lazarus Group is an umbrella term for North Korean state-sponsored cyber threat actor groups. The cyber operations conducted by North Korea's APT groups, such as the Lazarus Group, occur globally.

The Lazarus Group (APT38): In 2025, according to the FBI, a North Korean state sponsored APT group associated with the Lazarus Group and APT38 carried out the biggest cryptocurrency theft in history, stealing an estimated $1.5 billion in cryptocurrency because of its compromise of the ByBit cryptocurrency exchange. According to indictments announced by the U.S. Department of Justice in 2018 and 2021, members of the Lazarus Group were also responsible for carrying out the worldwide WannaCry ransomware attack in 2017 to fund the regime's activities.

The Lazarus Group (Famous Chollima): Famous Chollima, a subgroup of the Lazarus Group is linked to North Korea's IT worker infiltration scheme. In this scheme, DPRK nationals have posed as remote workers in U.S. and other Western companies under stolen or fabricated identities, primarily targeting information technology and technical roles. In some instances, these individuals have employed AI tools to generate synthetic identities and deepfake videos to pass online interviews. They generate revenue for the North Korean government, particularly to fund its weapons programs. In 2024, the U.S. Department of Justice (DOJ) indicted 14 North Koreans for their roles in this scheme, which is estimated to have generated over $88 million for the DPRK over six years. In January 2025, DOJ announced indictments against two U.S. citizens for operating a six-year scheme that placed North Korean operatives in over 60 U.S. companies. The NJCCIC assesses that the DPRK will continue to carry out cryptocurrency thefts, its IT worker infiltration scheme, and other revenue-generating cyber activities, as these cyber operations have proven to be lucrative and typically face minimal international repercussions.

Financially motivated cybercriminal organizations pose an immediate and persistent threat to New Jersey organizations and residents. These threat actors range from sophisticated ransomware syndicates conducting multi-million-dollar extortion campaigns to individual fraudsters executing social engineering schemes.

Ransomware

Ransomware remains the most financially and operationally destructive cyber threat facing New Jersey organizations. While there is no single authoritative source for the total number of ransomware victims in all of 2025, the New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) tracked over 8,000 ransomware attacks worldwide, representing a 31 percent year-over-year increase from 2024. Of the 2025 ransomware victims, more than 3,100 were in the U.S., including at least 48 public and private organizations in New Jersey. The top sectors targeted worldwide by ransomware groups were Manufacturing, Healthcare, Energy, and Government.

In 2025, multiple global law enforcement takedowns, indictments, and arrests disrupted several major ransomware groups and infrastructure. Despite these enforcement actions, the ransomware ecosystem and the number of victims continue to grow. In 2025, the ransomware landscape was dominated by groups such as Qilin, Akira, and Cl0p, that launched widespread global ransomware and data extortion campaigns, often by exploiting unpatched vulnerabilities or using compromised credentials to log in to victims' systems.

Notable 2025 Ransomware Incidents

Jaguar Land Rover: In late August and September, British automaker Jaguar Land Rover suffered one of the year's most disruptive cyberattacks. The threat actor group, Scattered Lapsus$ Hunters - who claimed credit for the attack in their Telegram channel - deployed ransomware that halted production across multiple plants for weeks, with broader supply-chain impacts and an estimated economic cost of over $2.5 billion. This cyberattack was one of the most economically damaging attacks in United Kingdom history and impacted its gross domestic product. The initial intrusion was enabled through social engineering tactics, including vishing (voice phishing) campaigns that tricked employees into disclosing credentials.

State of Nevada: In August, Nevada suffered a ransomware attack that effectively crippled all of its state government operations. The threat actor had infiltrated the system as early as May 14, when a state employee unknowingly downloaded a malware-laced system administration tool from a spoofed website. The attack disrupted over 60 state agencies including the Department of Motor Vehicles, the Supplemental Nutrition Assistance Program (SNAP) benefits program, and childcare programs. Nevada achieved recovery in 28 days at an approximately $1.5 million cost without making a ransom payment.

DaVita Healthcare: In April, DaVita, a major U.S. kidney dialysis provider, suffered a ransomware attack that encrypted parts of its network and led to the exfiltration of sensitive personal and health information for approximately 2.7 million patients. The attackers gained access to laboratory databases, exfiltrating up to 20 TB of data, including clinical results and Social Security numbers. DaVita reported $13.5 million in remediation and patient care costs related to the attack.

Maryland Transit Administration: In August, the Maryland Transit Administration (MTA), which is part of the Maryland Department of Transportation, suffered a ransomware incident that disrupted its MobilityLink paratransit system and real-time bus tracking. The attackers claimed to have exfiltrated sensitive data, including Social Security numbers, passports, and driver's licenses, demanding a $3.4 million (30 BTC) ransom. Maryland officials confirmed no ransom was paid and that core transit services, including local bus, metro subway, light rail, and Maryland Area Rail Commuter train service, continued operating normally. While the MTA's core services remained operational, some real-time information systems remained impacted for weeks. This incident underscores the risks to public transit infrastructure.

CodeRED Emergency Alert System: In November, CodeRED, an emergency notification system provided by Crisis24 and used for alerts about emergencies by law enforcement agencies and municipalities across the country (including at least 24 municipalities in New Jersey), suffered a ransomware incident that knocked the service offline nationwide for approximately two weeks. Additionally, the threat actor was able to steal user data, including names, addresses, email addresses, phone numbers, and passwords for user profiles. As a result of the damage caused by the attack, Crisis24 decommissioned the legacy platform and migrated all customers to a new secure environment.

Pennsylvania Office of the Attorney General: In August, the Pennsylvania Office of the Attorney General (OAG) confirmed a ransomware attack, also linked to the INC ransomware group. The breach, believed to have exploited the "Citrix Bleed 2" vulnerability, resulted in the exfiltration of sensitive legal and medical data. The OAG confirmed in November that the compromised personal information included names, Social Security numbers, and medical information. Although the OAG refused to pay the ransom and maintained its mission-critical functions, its website, email systems, and phone lines remained offline for about two weeks, and daily business operations were impacted for over a month.

Oracle E-Business Suite (EBS): Between July and October, the Cl0p ransomware/extortion group exploited a zero-day vulnerability in the Oracle E-Business Suite, exfiltrating data from nearly 30 major corporations, including victims such as Harvard University, American Airlines' subsidiary Envoy Air, and the Washington Post. Following the data thefts, Cl0p sent extortion emails to executives at the victim organizations with ransom demands in the tens of millions of dollars.

In summary, the NJCCIC assesses that in 2026, ransomware groups will continue targeting critical infrastructure systems and widely deployed enterprise software platforms. These attacks are expected to increase in number, resulting in debilitating operational impacts and costs to victims.

Cyber-Enabled Fraud Schemes

Just as ransomware attacks are typically financially motivated, cyber-enabled fraud is a growing threat, with losses by U.S. victims exceeding over $10 billion annually. Cyber-enabled fraud schemes have become increasingly sophisticated and prevalent, leveraging technology to deceive victims and steal money or sensitive information. The NJCCIC categorizes these schemes 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 of the cyber-enabled fraud schemes. In 2025, 59 percent (561) of the 954 incident reports submitted to the NJCCIC involved social engineering fraud schemes, including the following two types of examples:

SMS Scams (“SmiShing”): In 2025, scam text messages continued to proliferate, with attackers impersonating trusted entities to steal credentials or payment information from the public. Thousands of New Jersey residents received SMS scam text messages purportedly sent by the NJ Motor Vehicle Commission, NJ E-ZPass, and NJ courts claiming that the recipients must pay a fine. This scam was not unique to New Jersey. The FBI received over 60,000 complaints nationwide. According to security researchers at Resecurity and Palo Alto’s Unit 42 threat intelligence team, threat actors associated with a People’s Republic of China (PRC)-based organized crime group, the Smishing Triad, impersonated a wide array of state-specific toll collection services.

Affected systems included: E-ZPass in New Jersey, SunPass in Florida, FasTrak in California, and I-PASS in Illinois, among others. Victims received text messages impersonating state toll agencies, motor vehicle agencies, and court systems, claiming they owe unpaid road tolls and directing them to click a link to pay immediately. The text messages often threatened fines, legal action, or suspension of driving privileges if payment was not made by a certain date. The Department of Homeland Security estimates the Smishing Triad made over $1 billion from U.S. text scam victims over three years.

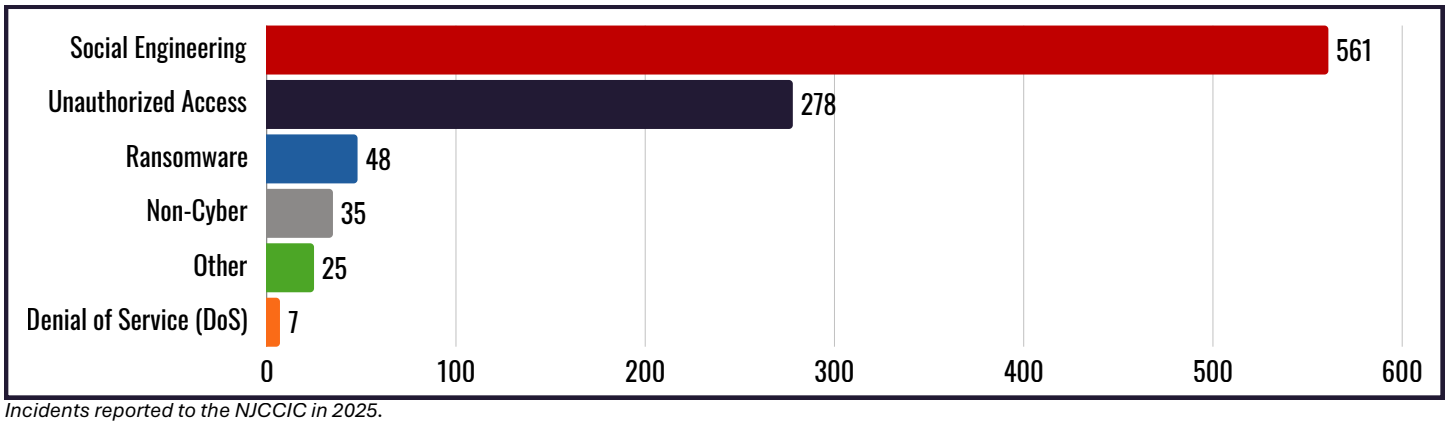
Pig Butchering Schemes (Romance/Investment Scams): Pig butchering is a sophisticated financial scam in which fraudsters cultivate trust with their victims over weeks or even months before luring them into fraudulent investments. The scheme often begins with friendly or romantic interactions on social 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 2025, a New Jersey resident reportedly lost over $280,000 to unidentified fraudsters in a pig butchering scam. Nationwide, U.S. victims lost more than $10 billion as a result of pig butchering scams.

In addition to the above examples, there are many more types of cyber-enabled fraud schemes, including business email compromise, tech support scams, employment scams, elder fraud, etc. Often, the themes of the scams are blended depending on the targets. The NJCCIC assesses that cyber-enabled fraud schemes will continue to grow in frequency and impact, with generative AI (GenAI) tools being employed to aid scammers in generating highly convincing personalized phishing emails, fake identities, deepfakes, and other deceptive content at scale, making it much easier to trick victims into sharing sensitive information or transferring money.

Beyond the immediate threats from nation-state adversaries and cybercriminals, several broader trends are reshaping the cyber threat environment in ways that will significantly impact New Jersey organizations in 2026 and beyond.

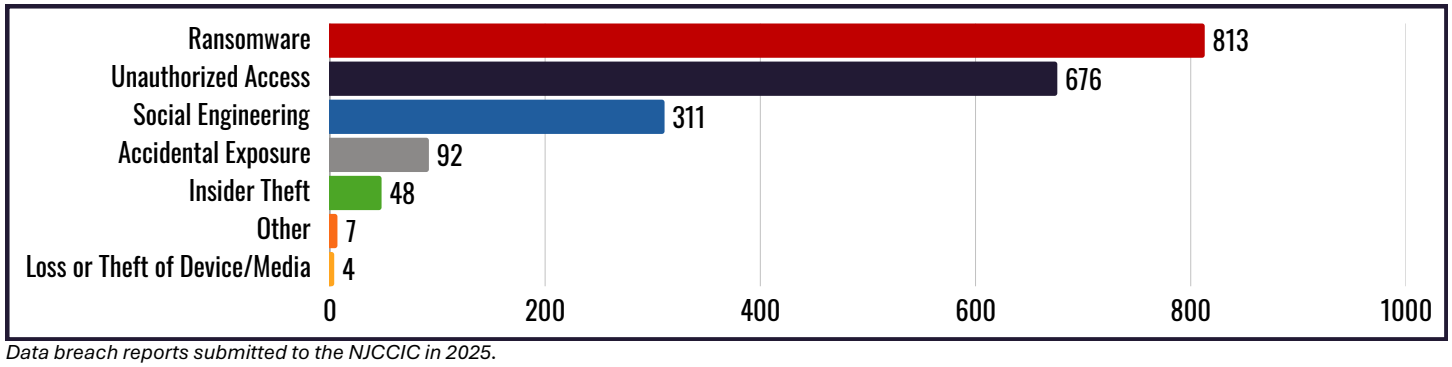
2025 Incident and Data Breach Reporting

In 2025, the New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) received 954 cybersecurity incident reports through its incident reporting portal (a 92 percent increase over 2024). Social Engineering (561) accounted for the majority of the reports to the NJCCIC, followed by Unauthorized Access/Hacking (278), and Ransomware (48).



Incidents reported to the NJCCIC in 2025.

Additionally, 1,951 initial data breach reports were submitted to the NJCCIC in 2025 from organizations across the U.S. whereby the breaches impacted New Jersey residents. The leading cause of data breach reports was ransomware attacks accounting for 42 percent or 813 of data breaches reported.



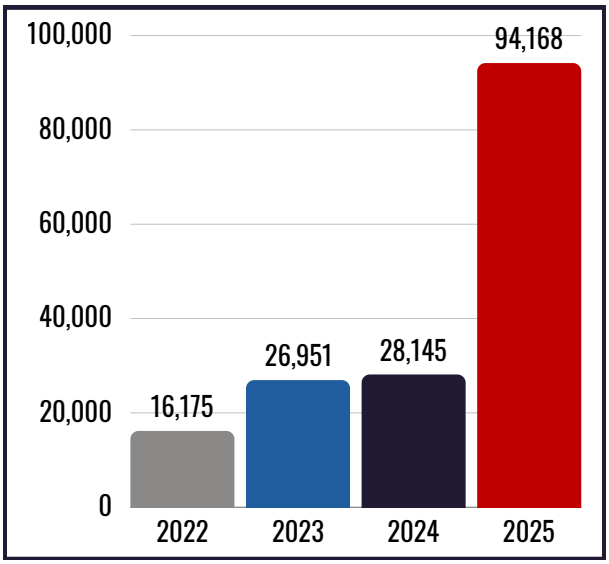
Data breach reports submitted to the NJCCIC in 2025.

Not all cyberattacks are reported to the NJCCIC. In addition to the reports made to the NJCCIC via its incident reporting portal, the NJCCIC also proactively notifies organizations whose information technology infrastructure has been compromised or whose networks contain vulnerabilities that threat actors could exploit. The NJCCIC sends proactive notifications due to indicators of compromise it detects, information provided by trusted third parties, and other open and commercial intelligence sources. In 2025, the NJCCIC notified 301 public- and private-sector organizations that their information technology infrastructure had been compromised. Thus, 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 proactive notifications to impacted entities.

The annual increases in incident reports submitted to the NJCCIC and the NJCCIC's proactive notifications to compromised organizations is expected to continue to grow in 2026 as more New Jersey residents become aware of the reporting service and the NJCCIC's threat hunting and analysis capabilities become more refined.

Compromised Credentials and Infostealer Malware

One of the most persistent and pervasive cyber threats heading into 2026 is the theft and abuse of login credentials. Compromised credentials, user IDs, and passwords that have been stolen or leaked are a key enabler in approximately 22 percent of cyberattacks according to the Verizon Data Breach Investigations Report (DBIR). The infostealer malware ecosystem that harvests credentials from infected computers continues to grow in scale. During 2025, threat actors obtained billions of usernames, passwords, and authentication tokens belonging to individuals and organizations, and they either traded or sold these credentials on underground markets. Compromised login credentials are a favored method for threat actors to gain unauthorized network access, often without detection, by appearing as legitimate logins. The NJCCIC's analysis of ransomware attacks conducted against New Jersey victim organizations found that compromised credentials were used to gain initial access in the majority of incidents. To mitigate risks associated with compromised credentials, the NJCCIC proactively monitors dark web marketplaces, paste sites, and other sources for exposed email and password combinations belonging to New Jersey public sector and critical infrastructure personnel. When credentials are discovered, the NJCCIC notifies the affected organizations and provides guidance on reducing the risk of misuse—including changing the compromised password on all accounts where it was used, using unique and long passwords for each account, implementing a password manager, enabling multifactor authentication (MFA), and installing anti-virus or endpoint detection and response (EDR) software.



Compromised credential notifications by year (2022-2025).

In 2025, the NJCCIC issued 94,168 compromised credential notifications, a 235 percent increase over 2024. 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 2026.

Artificial Intelligence (AI): From Enhancement to Autonomy

In 2025, the cybersecurity landscape moved beyond AI-generated phishing and deepfakes to the era of the autonomous attacker. While threat actors continued to use large language models (LLMs) to conduct research and reconnaissance on potential targets and create high-fidelity deepfakes and automated phishing messages at scale in support of their fraud schemes and influence operations, the most critical development was the rise of agentic AI. The emergence of agentic AI now allows threat actors to use reasoning models to orchestrate and automate the entire attack lifecycle at a speed and scale that outpace human-driven defenses.

In November 2025, Anthropic, a generative AI LLM provider, disclosed the first documented large-scale cyber-espionage campaign in which an AI-enabled agent conducted the majority of attack operations with minimal human oversight. A PRC-nexus state-sponsored threat actor used an agentic AI system to autonomously perform reconnaissance, identify vulnerabilities, generate exploit code, move laterally, harvest credentials, and exfiltrate data against dozens of global targets, with humans intervening only at a small number of key decision points.

This disclosure creates a major paradigm shift with respect to cybersecurity and the ability for organizations to defend against agentic AI attacks. Agentic AI transforms cyber threats from discrete, human-paced incidents into machine-speed, self-directed campaigns, making automation, collective defense, and resilience the defining priorities of cybersecurity in the years ahead.

Systemic and Supply-Chain Risk

The global cyber risk environment is increasingly shaped by systemic dependencies on cloud platforms, managed service providers, and third-party software. The concentration of critical services within a limited number of vendors creates single points of failure where outages, misconfigurations, or compromises can disrupt multiple sectors simultaneously.

In 2025, this risk was demonstrated by major cloud outages affecting all three dominant hyperscale providers, Amazon Web Services (AWS), Microsoft Azure, and Google Cloud, as well as content delivery networks such as Cloudflare. These outages caused cascading disruptions across government, healthcare, transportation, education, and private industry. Major consumer and enterprise platforms were also affected, including services such as Snapchat, Netflix, and Spotify, highlighting how failures in shared infrastructure can rapidly propagate across the entire digital ecosystem.

Software supply-chain attacks further amplify this risk by targeting trusted upstream components, including open-source libraries, SaaS integrations, and commercial software updates. By compromising a single vendor or dependency, threat actors can bypass perimeter defenses and gain access to numerous downstream organizations simultaneously. These attacks are difficult to detect because malicious activity is delivered through legitimate update mechanisms or authenticated vendor connections. Recent attacks against open-source repositories, including GitHub, the Python Package Index (PyPI), and the Node Package Manager (NPM) ecosystem, resulted in millions of downloads of malicious packages containing infostealer malware.

Commercial software supply chains were similarly targeted, as evidenced by the F5 breach documented above. This incident is reminiscent of the 2021 SolarWinds compromise, in which Russia's SVR inserted malicious code into a software update, gaining access to major enterprise networks across nearly every critical infrastructure sector.

The NJCCIC assesses that supply-chain attacks will increase in 2026 and beyond, as threat actors recognize that compromising upstream service providers grant access to not only the provider, but also to their entire downstream customer base.

IOT, OT, and Cyber-Physical Exposure

Internet of Things (IoT) and Operational Technology (OT) systems now play a central role in controlling physical processes across transportation networks, utilities, healthcare facilities, manufacturing environments, and public venues. Many of these systems were not designed with modern cybersecurity principles and often rely on outdated firmware, weak authentication, and limited monitoring. As a result, they are frequently internet-exposed and difficult to secure, expanding the state's cyberattack surface.

In 2025, U.S. and international incidents, as documented in the above sections, demonstrated how basic techniques, such as stolen credentials, default passwords, and unpatched remote access services, were used to access water systems, transportation controls, and industrial environments. Pro-Russian and pro-Iranian hacktivist groups conducted operationally disruptive attacks against critical infrastructure, highlighting the risk that exposed IoT and OT systems present. Further, as demonstrated in the Jaguar Land Rover ransomware incident, the convergence of IT environments with OT environments can have devastating consequences.

As the proliferation of IoT and OT systems continues to increase in 2026, the NJCCIC assesses that more attacks will target the vulnerabilities inherent in these systems.

Vulnerability Exploitation

The Cybersecurity and Infrastructure Security Agency's (CISA) Known Exploited Vulnerabilities (KEV) catalog serves as a critical prioritization tool for vulnerability management. The catalog contains vulnerabilities confirmed to have been exploited by threat actors, making them extremely high risk. In 2025, the KEV catalog grew by approximately 20 percent, with 245 vulnerabilities added—more than 30 percent above the previous two years' trend. The catalog ended 2025 with 1,484 entries. Of the vulnerabilities added, 24 were confirmed to have been exploited by ransomware groups.

Notable KEV Vulnerabilities Exploited in 2025 Attacks

CitrixBleed 2 (CVE-2025-5777): As documented in the Ransomware section above, the Pennsylvania OAG's office suffered a ransomware attack in which the CitrixBleed 2 vulnerability was the initial access point. Over 100 other organizations worldwide were compromised as a result of this vulnerability, including Boeing, Comcast, and the Dutch Public Prosecution Service. This critical vulnerability in Citrix NetScaler ADC and Gateway allows unauthenticated attackers to extract session tokens, enabling MFA bypass. Threat actors, including a Russian ransomware group and a suspected Chinese APT group, were observed leveraging the flaw. To help mitigate the risk of exploit, the NJCCIC proactively notified eight New Jersey organizations that their Citrix environments were vulnerable and to apply patches.

Microsoft SharePoint (CVE-2025-53770 / CVE-2025-53771): These two vulnerabilities, dubbed ToolShell, allows threat actors to chain them together to gain unauthorized access to unpatched on-premises Microsoft SharePoint servers. Chinese nation-state threat actors are linked to the exploits of these vulnerabilities. Public reports documented that over 400 organizations worldwide were compromised because of these vulnerabilities, including the U.S. National Nuclear Security Organization, Department of Homeland Security, the Florida Department of Revenue, and others. The NJCCIC determined that the SharePoint servers of two New Jersey State government agencies were also targets. However, immediate response actions prevented their compromise. To help mitigate risk of exploit, the NJCCIC proactively notified 14 New Jersey organizations that their on-premises SharePoint servers were vulnerable and to apply patches.

Oracle E-Business Suite (EBS) (CVE-2025-61882): As documented in the Ransomware section above, the Oracle EBS vulnerability was exploited by the Cl0p ransomware group. This pre-authentication remote code execution vulnerability became the entry point into dozens of Oracle EBS customers, including Harvard University, American Airlines, Cox Enterprises, the Washington Post, and others. To help mitigate risk of exploit, the NJCCIC proactively notified one New Jersey public-sector organization that its EBS environment was vulnerable and to apply patches.

While the number of KEV vulnerabilities continued to increase in 2025, the average time from vulnerability disclosure to exploitation has decreased from 32 days in 2022 to just five days currently. This trend implores organizations to integrate KEV monitoring into vulnerability management programs and prioritize KEV-listed flaws. The NJCCIC's pre-victimization notification program (PVNP) proactively monitors for and notifies New Jersey organizations of KEV vulnerabilities in their environments. In 2025, the NJCCIC made 240 PVNP notifications.

FIFA World Cup 2026: Cyber Threat Considerations

The FIFA World Cup 2026 will span 16 venues across the U.S., Mexico, and Canada, with matches running for 39 days from June 11 to July 19. MetLife Stadium in East Rutherford (Bergen County) will host eight matches including the tournament's final match.

Major international sporting events have become prime targets for cyber threat actors, as evidenced by attacks on the FIFA World Cup 2022 in Qatar, Euro 2024 in Germany, and the 2024 Summer Olympics in Paris.

FIFA World Cup 2022: About six months before the FIFA World Cup 2022, a PRC-linked threat actor breached the network of a major communications provider for the games and planted malware on a critical system storing network device configurations. This breach remained undetected until six months after the games and could have disrupted coverage. Threat actors and hacktivists also launched DDoS attacks on Qatar-based entities, such as qatargas.com and moci.gov.qa during the World Cup, while targeting fans with phishing campaigns, fake ticket sales, and malicious mobile apps.

Euro 2024: Euro 2024 saw thousands of phishing campaigns and more than 15,000 Union of European Football Association customer credentials were exposed on underground forums. A DDoS attack targeted Polish public television disrupting its online broadcast of Poland's opening match. This attack was later attributed to Russian threat actors.

2024 Summer Olympics: French authorities disclosed that the 2024 Summer Olympics faced more than 140 cyberattacks, including at least 22 incidents where malicious actors successfully gained access to information systems. The Grand Palais and several other museums throughout France were also targeted by ransomware attacks, while Russian groups used AI-generated content to create fake news and images aiming to discredit the International Olympic Committee and instill fear among potential attendees.

Across all three events, threat actors employed similar tactics of credential theft, phishing, distributed denial-of-service (DDoS) attacks, fake ticketing schemes, malicious mobile applications, and disinformation campaigns, with Russia-linked actors posing particularly elevated threats due to geopolitical grievances stemming from sanctions and athletic bans.

The NJCCIC assesses that the FIFA World Cup 2026 may potentially experience similar threat activity, ransomware, and nation-state targeting. Deepfake technology may be used for disinformation. Critical infrastructure supporting the World Cup may also be targeted, and modern stadium IoT systems present potential attack vectors.

As early as August 2025, the NJCCIC observed a surge in domain registrations tied to the upcoming FIFA World Cup 2026. These domains, often masquerading as legitimate ticketing portals, merchandise outlets, or live-stream platforms, serve as precursors to a multifaceted cyber campaign designed to harvest credentials, distribute malware, and siphon financial data.

The NJCCIC, in coordination with the New Jersey State Police, is leading cybersecurity preparations for the NY/NJ area ahead of the matches this summer. It is working in partnership with public- and private-sector organizations throughout the region, while also coordinating threat intelligence sharing with all host city cybersecurity teams in the U.S., Canada, and Mexico.

Changes in Federal Cybersecurity Support

In March 2025, the White House issued Executive Order 14239, "Achieving Efficiency Through State and Local Preparedness," which fundamentally rebalances cybersecurity roles across the nation. Whereas previous approaches positioned the federal government as the primary defender, the new model shifts primary responsibility for cyber preparedness, defense, and response to state, local, and private-sector entities, with federal agencies serving in a supporting and coordinating role. The defunding of the Multi-State Information Sharing and Analysis Center (MS-ISAC), the termination of the Cyber Safety Review Board, and the downsizing of CISA personnel, further underscores this shift.

In September 2025, both the State and Local Cybersecurity Grant Program (SLCGP) and the Cybersecurity Information Sharing Act of 2015 expired. While both programs were temporarily continued through January 2026, their long-term status is unknown.

Using SLCGP funds, the NJCCIC conducts continuous risk monitoring for more than 800 State and local government entities, including municipalities, counties, State organizations across the executive, judicial, and legislative branches, K-12 schools, State and county colleges and universities, and municipal utility authorities that provide water and wastewater services. SLCGP funds allow the NJCCIC to provide Endpoint Detection and Response (EDR) software and 24/7 Managed Detection and Response (MDR) services to 153 of the above organizations covering over 82,000 desktops, laptops, and servers. The EDR/MDR services have prevented over 200 ransomware incidents since its inception in 2023. In addition, using SLCGP funds, the NJCCIC has been able to provide 120 of the above listed organizations with more than 17,000 phishing-resistant MFA tokens. Without continued authorization of the SLCGP and sustained funding, the progress New Jersey has made in reducing cyber risk across State and local government will erode, significantly increasing the public-sector threat environment.

With the federal government stepping back from its traditional cybersecurity role and critical grant funding in limbo, New Jersey faces a 2026 threat landscape where hard-won protections for hundreds of public-sector entities may disappear.

Cybersecurity Conclusion

The threat environment facing New Jersey entering 2026 is defined by convergence: increasingly capable nation-state adversaries, highly resilient cybercriminal ecosystems, rapid adoption of AI-enabled attack techniques, and systemic dependencies on shared digital infrastructure. As this assessment demonstrates, cyber risk is no longer confined to data loss or service disruption, it now directly threatens public health and safety, economic stability, and public confidence in essential government and private-sector services. The acceleration of exploitation timelines, the expansion of supply-chain and cloud concentration risks, and the growing exposure of IoT and OT systems collectively mean that cyber incidents are more likely to cascade across sectors and jurisdictions simultaneously, amplifying their real-world impact. These challenges are further compounded by the contraction of federal cybersecurity support and uncertainty surrounding sustained grant funding, placing greater responsibility on State and local entities to defend increasingly complex environments.

Despite these challenges, New Jersey has made meaningful progress through centralized coordination, intelligence-driven risk reduction, and proactive engagement with public and private partners. Continued success in 2026 and beyond will depend on sustained investment in collective defense capabilities, rapid vulnerability mitigation, credential and identity protection, OT security, and resilience planning—particularly in preparation for high-profile events such as the FIFA World Cup 2026. By strengthening partnerships, maintaining situational awareness, and prioritizing resilience alongside prevention, New Jersey can reduce risk, limit the impact of inevitable incidents, and continue to protect the safety, prosperity, and trust of its residents in an evolving and complex threat environment.

RESOURCES

New Jersey Shield

New Jersey Shield is a collaborative effort between the New Jersey Office of Homeland Security and Preparedness (NJOHSP) and the New Jersey Regional Operations & 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

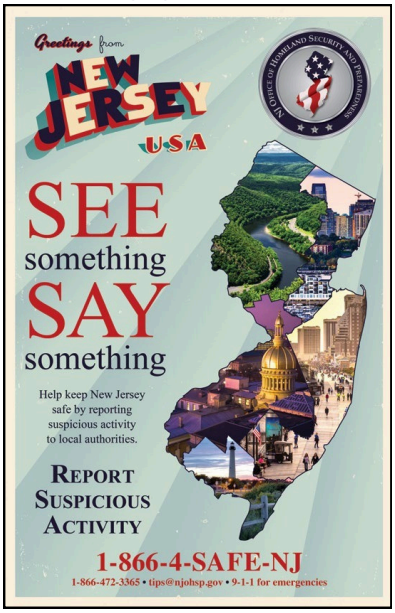
New Jersey is home to many organizations that operate on a national and global scale. By partnering with similar programs worldwide as part of a global network, New Jersey Shield meets the needs of its partners not only in New Jersey, but in other states in the U.S. and in countries across the world.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

Suspicious Activity Reporting (SAR)

The New Jersey Office of Homeland Security and Preparedness (NJOHSP) encourages law enforcement, first responders, private- and public-sector partners, and the public to report potential threats and suspicious activity related to terrorism, targeted violence, counterintelligence, or other related activity to support prevention efforts. Even small or seemingly insignificant observations can help complete a larger picture and help keep our communities safe.

Public Engagement



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 New Jersey Suspicious Activity Reporting: Recent 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 with law enforcement partners throughout the State. NJSARS is linked to the FBI's national 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, counterintelligence threats, 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

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

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

Cyberattack:
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)


NJ Office of Homeland Security and Preparedness

NEW JERSEY OFFICE OF HOMELAND SECURITY AND PREPAREDNESS