2024

Threat Assessment

New Jersey Office of
Homeland Security and Preparedness

njohsp.gov | cyber.nj.gov

NJ Office of Homeland Security and Preparedness

About Us

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

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

Mission

NJOHSP leads and coordinates New Jersey's counterterrorism, counterintelligence, cybersecurity, and preparedness efforts while building resiliency throughout the State.

Core Values

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

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

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

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

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

Foreword

The sudden and tragic loss of life since the start of the October 7 Israel-HAMAS conflict, along with its stateside ripple effects on extremism, serves as a stark reminder that we can never be too prepared, informed, or vigilant. The New Jersey Office of Homeland Security and Preparedness was engaged with other state and federal partners to assist in the safe passage of those citizens of New Jersey affected by the war. NJOHSP remains dedicated to countering and mitigating terrorism, foreign intelligence, and cyber threats while adapting to a dynamic threat landscape amid the ever-increasing capabilities of threat actors.

Looking ahead to 2024, NJOHSP analysts identify homegrown violent extremists (HVEs) and white racially motivated extremists (WRMEs) as the highest threats to New Jersey. While the threat from HAMAS and other foreign terrorist organizations (FTOs) is low, HVEs, inspired by these groups, may be motivated by global conflicts to plan or execute attacks in the U.S. Domestic extremists, including WRMEs, may exploit the upcoming presidential election to amplify their ideologies and commit acts of violence, focusing on soft targets like mass gatherings and critical infrastructure. Here in our home state, a collaborative effort between NJOHSP detectives and analysts led to the March arrest of a Toms River (Ocean County) domestic extremist who attacked individuals attending a January 2023 anti-racism concert at a church in Asbury Park (Monmouth County). There is also a possibility that domestic extremists will follow the emerging trend of threatening government officials.

As always, partnerships play a significant role in the safety and security of New Jersey, with one of our newer initiatives being the New Jersey Statewide Threat Assessment Team (NJ STAT). This joint effort between federal, State, county, and local agencies is designed to effectively identify, assess, and intervene as needed, providing an "off-ramp" to individuals who are at risk of conducting targeted acts of violence. It is the first time our state has worked in lockstep to incorporate case consultation, assessment, action plan support, and referral management to preemptively address potential violence.

In 2023, the New Jersey Cybersecurity and Communications Integration Cell documented over 4,100 ransomware attacks worldwide that were publicly listed on the respective threat actors' leak sites and elsewhere. The ransomware victim lists contained 60 New Jersey public and private sector organizations. These institutions, as well as its residents, face a consistent and credible threat of cyberattacks from multiple types of threat actors with varying capabilities and motivations. Nation-state actors, such as China, Russia, Iran, and North Korea have targeted American companies and infrastructure for espionage and potential disruption of critical systems.

In closing, we express gratitude to all our partners who contributed to NJOHSP's 2024 Threat Assessment. Our commitment remains unwavering in ensuring the safety and security of our State, its residents, and visitors. Recognizing the public as one of our first and best lines of defense in the fight against terrorism, I urge you all to stay vigilant and if you "See Something, Say Something" by reporting terrorism-related suspicious activity to NJOHSP's Counterterrorism Watch Desk at 866-4-SAFE-NJ and tips@njohsp.gov.

Sincerely,

Laurie R. Doran

Director, NJOHSP

February 2024

Table of Contents

Information Cutoff: December 31, 2023

New Jersey's Assessed Threat Level in 2024

2024 Assessed Threat Level

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

Detailed information on these extremist groups and individuals can be found at njohsp.gov/terrorism-snapshots.

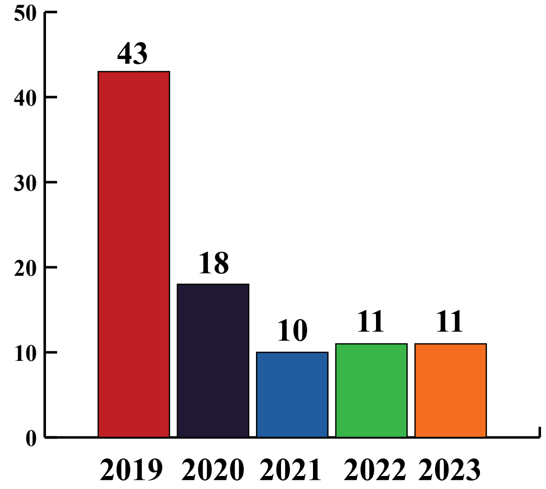
High Threats in 2024

Regional HVEs Unwavering in Commitment to Violence

Despite waning arrests, homegrown violent extremists (HVEs) remain a high threat due to their unwavering commitment to foreign terrorist organizations which encourage them to plot attacks within the United States. Over the last five years, 37 percent of HVE attacks and plots occurred in New Jersey and its surrounding states, further highlighting the sustained threat to this region.

In August, federal authorities arrested an unnamed male juvenile in Philadelphia on multiple charges stemming from an FBI Joint Terrorism Task Force investigation. The juvenile acquired chemicals and began constructing multiple improvised explosive devices (IEDs). He also stockpiled weapons and received 14 international shipments of military and tactical gear at his address. The juvenile communicated with a social media account associated with Katibat al Tawhid wal Jihad, a Syrian-based group affiliated with al-Qa'ida (AQ). AQ and its affiliates frequently advocate for attacks against "unbelievers" in support of their ideology and have distributed propaganda encouraging the construction and use of IEDs. In September, AQ issued a statement celebrating its network of supporters and members, including those "even from America," and claimed it was "planning for the next attack."

Identified HVEs by Year*



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

On December 31, 2022, Trevor Bickford traveled to New York City from Maine and attacked three police officers with a machete at a security checkpoint during New Year's Eve celebrations. Bickford allegedly became radicalized in the summer of 2022 and conducted the attack on behalf of the Taliban. Prior to the attack, in November 2022, Bickford told a family member he planned to travel to Afghanistan to join the group and become a suicide bomber. Authorities found a journal in Bickford's backpack with a message written on the day of the attack stating, "this will be my last entry." Furthermore, Bickford wrote that his brother, who joined the U.S. military, had "joined the ranks of the enemy."

In November 2022, authorities arrested Omar Alkattoul of Sayreville (Middlesex County) for using social media to share a manifesto in which he threatened to attack a synagogue. His manifesto, titled "When Swords Collide," contained hateful rhetoric aimed at the Jewish community and stated that he would target a synagogue and that "many more attacks like these… will come." Alkattoul also recorded himself pledging allegiance to ISIS and its recently deceased leader at the time, Abu al-Hassan al-Hashimi al-Qurayshi, during which he promised to "obey [al-Qurayshi] during hard times and good times." During his arrest, he stated that he "identified with the ideologies of ISIS and al-Qa'ida" and reiterated his desire to blow up a synagogue. Alkattoul pleaded guilty in July and was sentenced to 15 months in prison in November.

Domestic Response to HAMAS Attack

On October 7, HAMAS launched an attack on Israel and killed more than 1,300 people, resulting in the deadliest terrorist attack against the nation since its founding. HAMAS' actions led to increased attention from international media as well as world leaders. While the threat to the U.S. from HAMAS is low, in 2024, HVEs may find inspiration from HAMAS and seek to commit violence in support of its actions. For example, in December, authorities arrested Karrem Nasr of Lawrenceville (Mercer County) in Kenya after he attempted to join al-Shabaab in Somalia. The attacks in Israel motivated Nasr's decision to travel.

HVEs: 2023 Regional Arrests

Victoria Jacobs | New York, New York

In January 2023, authorities arrested Victoria Jacobs for allegedly using cryptocurrency to provide financial support to Hay'at Tahrir al-Sham (HTS). Jacobs allegedly gave more than $5,000 to a terrorist training group affiliated with HTS and laundered over $10,000 on behalf of the group using cryptocurrency and gift cards. Jacobs provided U.S. military manuals to groups she believed to be associated with HTS and al-Qa'ida-affiliated Hurras al-Din to assist their bomb-making abilities.

Ridon Kola | Yonkers, New York

In March, police arrested Ridon Kola after he posted multiple messages online threatening to kill police officers and the Yonkers' mayor during St. Patrick's Day festivities. From November 2021 until his arrest, Kola posted a variety of threats online against the Yonkers Police Department. In some of the posts, Kola referenced his support for ISIS and Sayfullo Saipov, the HVE who killed eight and injured 11 in the 2017 NYC vehicle ramming attack on Halloween.

Kamal Fataliev | Philadelphia, Pennsylvania

In July, authorities arrested Kamal Fataliev for making false statements to federal agents. Fataliev allegedly posted more than 200 bomb-, poison-, and weapon-making manuals online and gave them to individuals he believed to be ISIS members. Fataliev also provided support to an FBI-cooperating individual posing as a potential plotter to whom he offered techniques for purchasing bomb-making materials.

Unnamed Juvenile | Philadelphia, Pennsylvania

In August, federal authorities raided the home of an unnamed juvenile in Philadelphia after uncovering his attempted support of the al-Qa'ida-affiliated group, Katibat al Tawhid wal Jihad (KTJ). The juvenile allegedly communicated with KTJ overseas and exchanged media containing terrorist propaganda and guidance on committing criminal acts. The juvenile researched potential attack targets while maintaining a "significant number" of firearms, tactical equipment, and items used for remote detonators.

Karrem Nasr | Lawrenceville, New Jersey

In December, authorities arrested Karrem Nasr in Kenya while he was traveling to Somalia to join al-Shabaab, the al-Qa'ida affiliate in the region. In November, Nasr began communicating online with an individual he believed could help him join al-Shabaab, but who was an undercover law enforcement agent. Nasr told the individual he had been thinking about engaging in jihad for a long time and was motivated by the October 7 HAMAS terrorist attack in Israel.

WRMEs Dedicated to Harassment and Attacks on Soft Targets

In 2024, white racially motivated extremists (WRMEs) will focus on attacking soft targets due to high casualty potential as well as writing and posting hateful rhetoric online to share their motivations with like-minded individuals and threaten their perceived enemies. Over the past five years, WRMEs conducted attacks resulting in the highest number of fatalities at soft target locations with 51 individuals killed and approximately 53 injured.

In May, Mauricio Garcia opened fire at an outlet mall in Texas, killing eight individuals and wounding seven others. Responding police later shot and killed the gunman. Weeks before and just prior to the attack, Garcia espoused antisemitism and support for Nazi ideology online, referencing the "replacement theory," while sharing many images of his firearms and of the outlet mall. After the attack, authorities discovered a Right-Wing Death Squad patch, affiliated with WRMEs, on his tactical gear along with several other weapons in his vehicle. Garcia also had over 100 pages of a written diary detailing his hatred toward several races that was uploaded to a Russian social media site.

In August, Ryan Palmeter fatally shot three black individuals and then himself at a retail store in Jacksonville, Florida. He was armed with a handgun and a rifle painted with swastikas. During the attack, Palmeter texted his father and asked him to break into his room where he left a suicide note, a will, and multiple manifestos which included violent racially motivated extremist content. Authorities believe he specifically targeted members of the black community based on the items found at his residence. Prior to the attack, Palmeter filmed himself wearing a tactical vest and gloves at a historically black university where a security guard saw him and alerted a nearby police officer.

Images Mauricio Garcia posted to his social media prior to the attack.

In 2023, authorities arrested two WRMEs for posting separate threatening messages online targeting Volusia County, Florida Sheriff Mike Chitwood. In March, police arrested Richard Golden, a New Jersey resident, for writing a death threat, claiming he would kill Chitwood after the sheriff denounced a WRME group for spreading fear and antisemitic hate literature in a Jewish community. Golden urged online supporters to murder Chitwood with a firearm to "solve an immediate problem permanently." Also in March, Joshua Wahl, a resident of Alaska, allegedly sent threatening emails and posted messages online calling on his supporters to harm the sheriff. Both individuals used chat rooms notorious for extremist content.

Mainstream WRME Ideology

Accelerationism is a theory that Western governments are corrupt and their demise should be accelerated through political tensions to create radical social change. Some WRMEs embrace a violent form of accelerationism as a way of establishing a whites-only ethnostate.

The Great Replacement Theory is the belief that the white race will become extinct due to forced assimilation, non-European immigration, and interracial marriage. Some WRMEs use this belief to spread the fear that their race will lose its superiority if supporters do not join them.

Domestic Terrorism

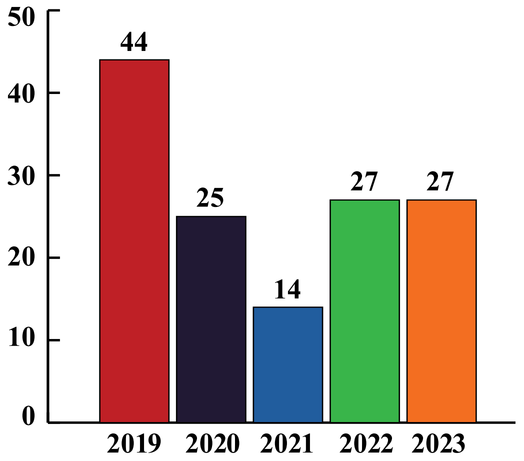
Domestic Terrorism Overview

In 2023, domestic extremists attacked soft targets, threatened Jewish communities, and coordinated with like-minded extremists to intimidate their perceived enemies. Among the 33 extremists identified, 28 were arrested, two took their own lives after an attack, and three engaged in a fatal confrontation with law enforcement.

In four unrelated attacks, white racially motivated extremists conducted a fatal shooting at a Texas outlet mall, as well as a Florida retail store and used incendiary devices to target two houses of worship. One abortion related extremist used an incendiary device to damage an abortion provider, while two anarchist extremists used smoke bombs and fireworks to attack a crowd that was waiting to enter a public event at the University of Pittsburgh.

In June, Seann Pietila of Pickford, Michigan, was charged in a three-count indictment for threatening to attack a synagogue on the fifth anniversary of the 2019 New Zealand mosque attacks. He allegedly made threats on social media which included comments about neo-Nazi ideology, antisemitism, and glorifying mass shootings. When authorities arrested Pietila at his home, they discovered a cache of weapons, knives, tactical equipment, a red-and-white Nazi flag, and makeshift plans for killing members of the congregation.

Incidents by Year*

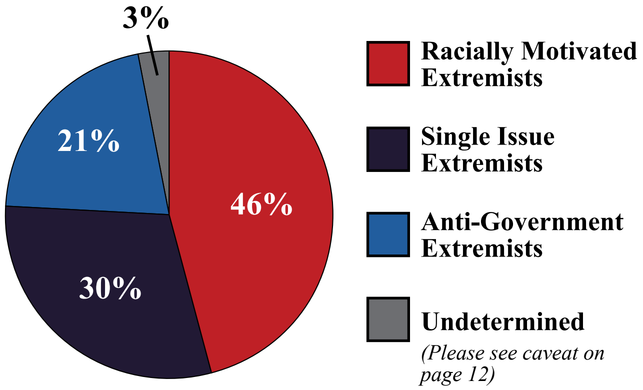


**This data only reflects publicly available information related to domestic terrorism incidents nationally and may be subject to change.*

In 2023, one-third of all arrested extremists coordinated with another subject to intimidate their perceived enemies. In two separate incidents, two or more subjects used an incendiary device to attack a soft target while three anarchists released public information belonging to a law enforcement officer. In another incident, two subjects from different states plotted to attack several electrical substations in the Baltimore area.

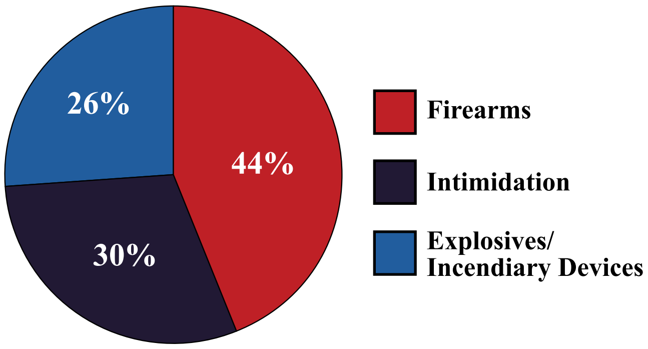
Domestic terrorism is violence committed by individuals or groups primarily associated with U.S.-based movements, including anti-government, racially motivated, religious, and single-issue extremist ideologies.

Ideological Affiliation



(Please see caveat on page 12)

Methods Used in Incidents



2023 Domestic Extremism Attack Timeline

January 13

Sovereign Citizen Extremist: Jada Davis shoots at a police officer in St. Louis, Missouri, after refusing to move her vehicle outside a Social Security building. She fires from inside her van after the officer breaks her window to remove her from the vehicle. Davis said she does not have a contract with the U.S. government and therefore does not have to follow its laws.

January 15

Abortion-Related Extremist: Tyler Massengill uses an incendiary device to damage an abortion health clinic in Peoria, Illinois. He initially denied responsibility for the arson but ultimately admitted to breaking a window and placing a burning container inside the building. Massengill received 10 years in prison followed by three years of supervised release and was ordered to pay $1.45 million in restitution.

January 27

White Racially Motivated Extremist: Nicholas Mucci attacks attendees at an anti-racism concert at Trinity Episcopal Parish in Asbury Park (Monmouth County). While yelling, "White lives matter, too," Mucci attempts to block concertgoers from leaving the event and throws multiple smoke bombs toward the church before driving off.

March 25

White Racially Motivated Extremist: Aimenn Penny uses a Molotov cocktail to burn down the Community Church of Chesterland, Ohio, in protest of two drag events. Authorities discover at Penny's residence "a handwritten manifesto that contained an ideological statement, a Nazi flag, Nazi memorabilia, a White Lives Matter of Ohio T-shirt, a gas mask, multiple rolls of blue painter's tape, and gas cans."

April 18

Anarchist Extremists: Brian DiPippa ignites and drops two homemade smoke bombs into a crowd waiting to enter an event at the University of Pittsburgh. Krystal DiPippa ignites and throws a large firework into a group of police officers causing a loud explosion that injures several officers. Law enforcement discover a red and black diagonally divided flag, which is associated with anarchist extremists, at their residence.

2023 Domestic Extremism Attack Timeline

May 6

HATE

White Racially Motivated Extremist: Mauricio Garcia kills eight people and injures seven at an outlet mall in Allen, Texas. Garcia arrives at the mall with three guns and a tactical vest and begins firing his rifle in the parking lot before entering the complex. A responding police officer shoots and kills Garcia during the attack. Following the incident, authorities discovered a WRME-affiliated patch on his tactical gear along with weapons and ammunition in his vehicle.

August 23

Sovereign Citizen Extremist: William Hardison shoots at sheriff deputies in Pittsburgh as they attempted to serve him with an eviction notice at a house where he had been squatting. Hardison barricades himself inside, shoots down police drones, and exchanges fire with officers before he's fatally shot. Harrison had stockpiled a supply of weapons and ammunition that prolonged the standoff. In 2019, Hardison described himself as a Moorish sovereign who rejects the laws of the U.S.

August 26

HATE

White Racially Motivated Extremist: Ryan Palmeter shoots and kills three employees at a retail store in Jacksonville, Florida. Palmeter arrives at the store wearing a tactical vest, face covering, and ear protection, and armed with a handgun and a rifle painted with a swastika. He kills his first victim in the parking lot and enters the store where he fatally shoots two other victims before killing himself.

November 20

HATE

Undetermined*: Benjamin Jones opens fire at a retail store in Beavercreek, Ohio, shooting and injuring four shoppers. When authorities responded to the scene, they discovered Jones dead from a self-inflicted gunshot wound. Racially motivated extremist ideology may have "at least partially" inspired Jones' attack based on evidence collected from his residence which included journal writings.

**The appropriate threat category has not yet been determined, as the attack is still under investigation to examine the subject's background, motives, connections, and online activity.*

Domestic Extremists Leverage Intimidation Tactics

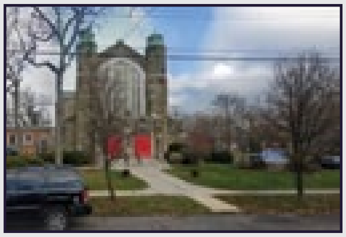
Domestic extremists with varying ideologies will participate in counterprotest demonstrations, engage in doxxing campaigns, and vandalize public and private property. Rather than conduct lethal attacks, supporters have relied on these tactics to motivate others to engage in similar criminal activities.

In October, approximately 25 members of the National Socialist Club (NSC-131), a New England-based neo-Nazi group, demonstrated outside the Massachusetts governor's home to protest immigration. Supporters chanted, "New England is ours; the rest must go." In July, five members of Patriot Front, a white racially motivated extremist group, were convicted of conspiracy to riot when members from approximately 10 states were arrested in June 2022, for planning to intimidate participants at an Idaho Pride event. Police discovered riot gear, a smoke grenade, shin guards, and shields after pulling over and searching their van. Officials have prosecuted the 31 members in smaller batches, citing the difficulties of having them all in one courtroom. In April, over a dozen NSC-131 supporters held a rally in Portland, Maine, making Nazi salute gestures while holding a banner that read, "Defend White Communities." The rally concluded with a physical altercation between demonstrators and counter-protesters.

In May, authorities arrested and charged three anti-fascist (Antifa) anarchist extremists, who opposed the construction of an Atlanta police training center, with harassment and misdemeanor stalking of an Atlanta police officer, who had previous involvement in a fatal shooting of a group member. The three suspects reportedly distributed flyers containing the officer's personal information and residential address. In March, Atlanta police arrested 23 suspects for vandalizing and burning equipment at the center's construction site. While using black bloc tactics, members threw commercial-grade fireworks, Molotov cocktails, large rocks, and bricks at police officers. Nationwide, supporters have smashed windows and vandalized businesses to intimidate and punish those proprietors and staff who are affiliated with the Atlanta Police Foundation and who support the construction of the police facility.

Since 2022, abortion-related extremists have threatened their opponents by vandalizing abortion clinics, pregnancy centers, and religious institutions. In June, law enforcement arrested Tibet Ergul and Chance Brannon for firebombing a California abortion clinic in March 2022. Both suspects conducted surveillance, obtained materials, and assembled the device. A third suspect, Xavier Batten, was arrested in July for allegedly advising and directing Brannon on how to construct a Molotov cocktail. A federal grand jury indicted the suspects with conspiracy and malicious destruction of property using fire and explosives. Brannon and Ergul are both charged with possessing an unregistered destructive device and one misdemeanor count of damaging a reproductive health service facility.

Case Study: Nicholas Mucci



Trinity Episcopal Parish in Asbury Park (Monmouth County).

In March, authorities arrested New Jersey resident Nicholas Mucci for attacking attendees at an anti-racism concert on January 27, 2023 at the Trinity Episcopal Parish. While yelling, "White lives matter, too," Mucci attempted to block concertgoers from leaving the event and threw multiple smoke bombs toward the church before driving off. Mucci returned later, exited his vehicle, and attempted to pepper spray the remaining attendees while again shouting, "White lives matter." During the investigation, authorities found that Mucci purchased the smoke bombs from a fireworks store in Pennsylvania.

Domestic Extremists Construct Various Weapons

Domestic extremists exploit the ease of constructing homemade weapons to attack and threaten their perceived enemies in furtherance of their prescribed ideologies. In 2023, extremists who identify with differing ideologies constructed ghost guns, incendiary, and explosive devices.

Abortion-Related Extremist **(ARE)**	In March, authorities arrested Hridindu Sankar Roychowdhury at Boston Logan International Airport in Massachusetts for his alleged part in constructing a Molotov cocktail to firebomb a Wisconsin Family Action office in 2022. Police discovered a burnt mason jar under a broken window and another jar filled with an accelerant. The exterior of the building contained spray painted messages saying "if abortions aren't safe then you aren't either." Another wall contained the anarchist symbol "A" representing anarchy inside the letter "O," which stands for order. Together, these symbols mean "society seeks order in anarchy."
Anarchist Extremists	In June, Brian and Krystal DiPippa disrupted an event at the University of Pittsburgh using homemade smoke bombs and large fireworks. Law enforcement found a red and black diagonally divided flag, which is associated with anarchist extremists, at their residence. Prosecutors indicted the couple on charges of conspiracy and obstruction of law enforcement.
Anti-Government Extremist **(Boogaloo Movement)**	In February 2023, law enforcement in Springfield, Missouri charged Timothy Zegar, who has ties to the Boogaloo movement, with trafficking and being a felon in possession of firearms. Law enforcement seized several pounds of a binary explosive and material used to construct improvised explosive devices (IEDs), 11 guns, a silencer, more than 1,000 rounds of ammunition, and body armor plates.
Sovereign Citizen Extremist	In March, police in American Canyon, California arrested Eddy Perez, a self-professed sovereign citizen, after leading officers on a car chase and discarding his ghost gun out of the driver side window. Perez was initially pulled over for having an illegal license plate. During a search of his home, authorities discovered five more firearms, including ghost guns and a bullet proof vest. Perez also had prior charges that restricted him from possessing a firearm.
White Racially Motivated Extremist (WRME)	In March, Aimenn Penny used two Molotov cocktails to attack the Community Church in Chesterland, Ohio. Penny allegedly tried to burn down the church in protest of two drag events scheduled to take place at the site. Penny was charged with one count of using fire to commit a federal felony, one count of malicious use of explosive materials, and one count of possessing a destructive device.

2024 Domestic Extremists Emerging Election Grievances

In 2024, domestic extremists – primarily anarchist, anti-government, and racially motivated – will exploit the presidential election to amplify their hostility towards social and economic policies, immigration, and ethnic and religious minorities. Domestic extremists' aversion to elections and democracy while embracing accelerationism, anarchy, and racial segregation will incite supporters to plot violent counter protest demonstrations, threaten government officials, and target critical infrastructure, including soft targets.

Anti-fascist (Antifa) anarchist extremists will reject both political parties and target politicians who they perceive as supporting law enforcement, border security initiatives, and Israel. They will also label corporate businesses and financial institutions as environmental criminals who discount climate change and other initiatives that seek to protect the environment. Based on past events, supporters using black bloc tactics to conceal their identity will threaten and vandalize campaign headquarters, financial institutions, and law enforcement offices while lone offenders will rely on homemade incendiary devices to conduct arson attacks. Online supporters will utilize doxxing methods to release home addresses of political candidates, law enforcement, and business owners while espousing antisemitic rhetoric and threatening Israeli supporters and Jewish communities. Demonstrators will also co-opt peaceful demonstrations, political events, and or challenge opposing extremist groups they consider fascists.

The purpose of this report is to identify the intent of domestic extremists to exploit the 2024 election. These potential threats were derived after reviewing open-source reporting, extremist propaganda, intelligence products, and **NJOHSP's 2020-2021 Supplemental Threat Assessment** located at: https://www.njohsp.gov/analysis/2020-2021-supplemental-threat-assessment

Anti-government and militia extremists will engage in violent counter-protest demonstrations to challenge Antifa and perceived political opponents. Lone offenders who distrust government institutions, subscribe to various conspiracy theories, and advocate for a second civil war will likely target and or vandalize polling locations, ballot drop boxes, and or plot attacks against campaign offices and government buildings. Online supporters who spread violent propaganda will call for federal law enforcement officers, election officials, and politicians to be arrested, prosecuted, and or executed. Conspiracy theorists will spread falsehoods about antisemitism, martial law, gun confiscations, immigration policies, and U.S. military intervention in Ukraine and Israel.

White racially motivated extremists (WRMEs) will spread disinformation and alter online propaganda to focus their efforts on disrupting the presidential election. Propaganda efforts will include WRMEs disparaging democracy as an external threat to the white race and suggest both presidential candidates and parties are beholden to Israel. Similar to WRMEs exploiting the Israel/HAMAS conflict, extremists will openly advocate for violence against the Jewish community by justifying their attacks as a "war for existence." Accelerationists will encourage attacking, creating chaos, disrupting election efforts, and calling for the killing of members of political parties and other government officials. WRMEs will amplify training efforts, banner displays, and other forms of propaganda during the election season to entice like-minded supporters to join their cause and fight back against their perceived enemies. Leading up to the election and after a candidate is chosen, WRMEs will partake in public marches, riots, and violence at designated locations to include soft target sites that present an opportunity for a mass casualty event.

Foreign Terrorist Organizations

Al-Qa'ida Emphasizes Affiliate Operations and Global Network

In 2024, al-Qa'ida (AQ) will promote its alleged network of global members and spotlight the successes of its affiliates' operations to emphasize its influence and commitment to attacks despite its reduced activity in the Middle East and the United States. In 2021, the U.S. Department of State's Country Terrorism Report indicated that AQ's core strength, in terms of fighters, was "seriously degraded" while its affiliates are engaged in frequent skirmishes in conflict zones throughout Somalia, sub-Saharan Africa, and South Asia.

In September, AQ published the 11th issue of its Arabic edition of *One Ummah* magazine in which it claimed the group had supporters and personnel "in its ranks from all over the world," including from India, Africa, "and even from America, Europe, and Russia." The group stated it had "cultural and international diversity" among its members, including "hundreds of specialists and professionals" and that it is "planning for the next attack," which will be "broader in impact and scope" than the 9/11 attacks. At the same time, the group acknowledged that it has to work to "regain many times" their losses in terms of regional "security havens" in the last two decades.

AQ issued a statement in June in which the group commented on activities in Africa perceived to be anti-Muslim. The group referenced the destruction of mosques for urban planning purposes as justification for waging jihad and supporting al-Shabaab, which is AQ's Somalian affiliate. AQ praised the group and claimed it is "the most experienced" and best option to defend Islam in East Africa. In February 2023, government leaders from Somalia, Ethiopia, Djibouti, and Kenya met to discuss the military offensive against al-Shabaab and, in response, AQ expressed support and more praise for al-Shabaab. It claimed the group had successfully fought off attempts by "crusader occupiers" to destroy its strongholds in the country and urged supporters to stand with the Somalian affiliate, which is "defending the land of their forefathers."

The U.N. Security Council released a July 2022 report that affirmed AQ's own rhetoric regarding its network and affiliates. The report stated a threat multiplier of AQ and other foreign terrorist organizations is its influence on foreign terrorist fighters and the "legacy of the 'caliphate'" which is passed down from group members to their dependents. It also stated that the international context "is favorable to al-Qa'ida, which intends to be recognized again as the leader of global jihad." The report confirmed the threat from AQ remains low in non-conflict zones but is "much higher in areas directly affected by conflict or neighboring it," such as Africa and Central and South Asia. Another AQ affiliate, Jama'a Nusrat ul-Islam wa al-Muslimin, is "increasing… control and expanding toward the Atlantic coast" while al-Shabaab is "exploiting political instability" and committing "attacks on high-level targets."

The Status of Al-Qa'ida's Leadership

In July 2022, the U.S. killed former AQ leader Ayman al-Zawahiri in Afghanistan. Neither AQ nor its affiliates have formally acknowledged his death. Despite the absence of official confirmation, the U.N. released a report in February 2023, based on member state intelligence, that identified the new de facto leader of AQ as Saif al-Adel.

Saif al-Adel

Al-Adel is an Iran-based senior AQ leader, who was previously a former Egyptian special forces officer. He took over as military commander of AQ following the death of Mohammed Atef during a U.S. airstrike in Afghanistan in November 2001. Prior to that, he taught militants to use explosives and trained some of the hijackers involved in the 9/11 attacks. Al-Adel is wanted by the FBI in connection with the August 7, 1998, bombings of the U.S. embassies in Tanzania and Kenya.

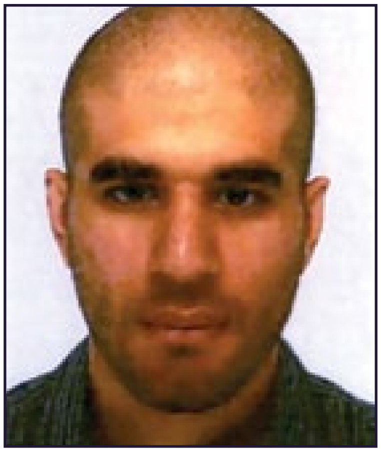
Global Pressure Keeps ISIS Threat to Homeland Low

As it continues to face pressure from opponents both locally and globally in 2024, ISIS will focus on the regional operations of its various affiliates and highlight its successes in an effort to reenergize its support base and motivate homegrown violent extremists (HVEs) to commit violence on its behalf. ISIS inspired eight of eleven (73 percent) HVEs arrested in 2023. In the last five years, ISIS-inspired HVEs constituted 76 percent of all HVE arrests, indicating that ISIS's reach, particularly in the U.S., has remained persistent despite its overall weakening.

In October, Ian McCary, deputy special envoy for the Global Coalition to Defeat ISIS, stated in an interview that "the fight is not yet done," even though ISIS has lost most of its territory in Iraq and Syria and tens of thousands of fighters. McCary said that despite ISIS's losses and its lack of control in Iraq and Syria, the group is still very active in the Sahel and West Africa, which is where the coalition is focusing its efforts. McCary claims that a contributing factor in any foreign terrorist organizations' (FTOs) success in Africa is due to "serious governance challenges" in parts of the continent where officials see "other actors move in and seek to exploit that void." Throughout 2023, ISIS supporters highlighted successful operations in Africa and the Khorasan region via its official and unofficial media outlets to increase its appeal to potential supporters.

Abdesalam Lassoued

Throughout the last year, ISIS, in its *al-Naba* newsletter and other publications, praised successful operations that resulted in terror attacks and encouraged supporters to remain dedicated. In *al-Naba's* 409th issue, ISIS encouraged its supporters to "take pride in the deeds and heroism of the soldiers of the caliphate." ISIS is attempting to reinvigorate its supporter base amid defeats and lack of global successes. The message shows empathy for its fighters' sacrifices while at the same time claiming it is resilient and dedicated to its goals. ISIS released similar messaging in its 399th issue in July when it compared its supporters to their ancestors and claimed that for every failure it encountered its enemies have experienced even greater setbacks.



Armand Rajabpour-Miyandoab

In October, ISIS claimed responsibility for a shooting in Brussels, Belgium, that left two dead and one injured. After the attack, the perpetrator, Abdesalam Jilni Meftah Lassoued, recorded a video claiming he was an ISIS fighter. In the 413th issue of *al-Naba*, ISIS celebrated the attack, claiming it "restored the atmosphere of terror for the crusaders from the lone wolf attacks of the mujahideen." ISIS also called for supporters to kill Jewish individuals around the world, including the U.S. and at Western embassies, in response to the HAMAS attacks against Israel on October 7. In December, Armand Rajabpour-Miyandoab killed a tourist with a knife and hammer in Paris. French authorties arrested Rajabpour-Miyandoab after he fled the scene. Before the attack, Rajabpour-Miyandoab recorded a video of himself pledging allegiance to ISIS and its leader Abu Hafs al-Hashimi al-Qurashi and calling for "Allah the Great to protect you, make you firm, and grant you victory over the enemies of the religion." The video was released shortly after he conducted the attack.

Social Media

Domestic and Homegrown Violent Extremist Use of Social Media

This assessment evaluates 27 domestic extremist attacks, plots, and threats from January 1, 2023, to December 31, 2023. Of the 27 domestic incidents, 13 had a social media nexus. These attacks were perpetrated by 14 individuals associated with white racially motivated and anti-government extremist ideologies.

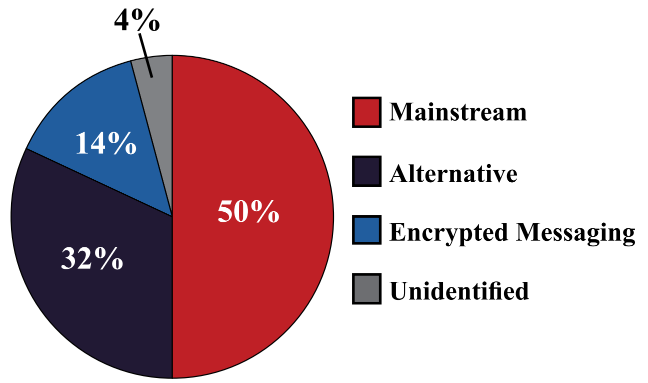
This assessment also identifies trends and patterns of eleven homegrown violent extremists (HVEs) who made threats and provided material support to foreign terrorist organizations (FTOs) from January 1, 2023 to December 31, 2023. All identified HVE cases in 2023 had a social media nexus.

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

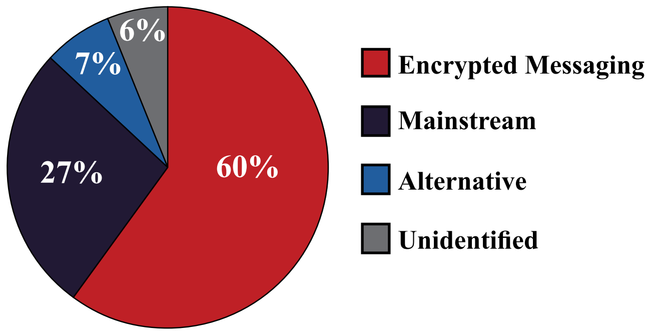
Threat Summary

An NJOHSP review of domestic extremist and HVE utilization of social media yielded notable statistics and trends, including platform type, pre-operational online activity, and ideological affiliation or group influence. Twelve out of 14 domestic threat actors identified with white racially motivated extremist (WRME) ideology. They predominately operated on mainstream platforms to discuss their ideologies and post threats, which accounted for 45 percent of their online activity. Smaller percentages used these platforms to view propaganda and plan attacks. HVEs used encrypted messaging platforms in 60 percent of the identified cases. They predominately used social media platforms to provide material support to FTOs, accounting for 33 percent of their usage. Smaller percentages used these platforms to discuss their ideology and post threats.

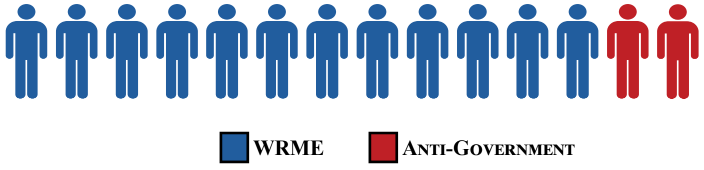
Domestic Extremist Platform Breakdown



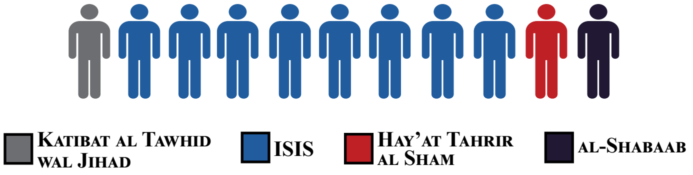
HVE Platform Breakdown



Domestic Extremist Ideology

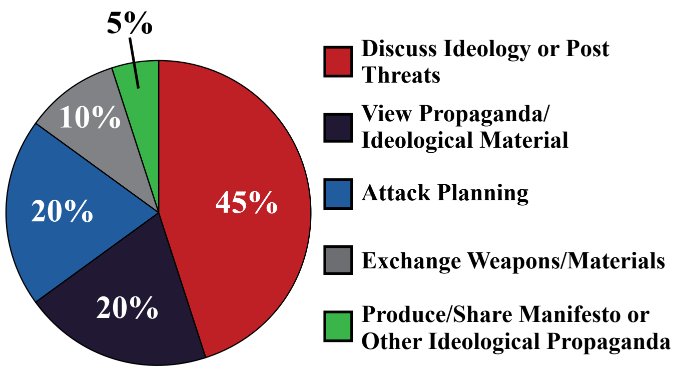


HVE Group Affiliation

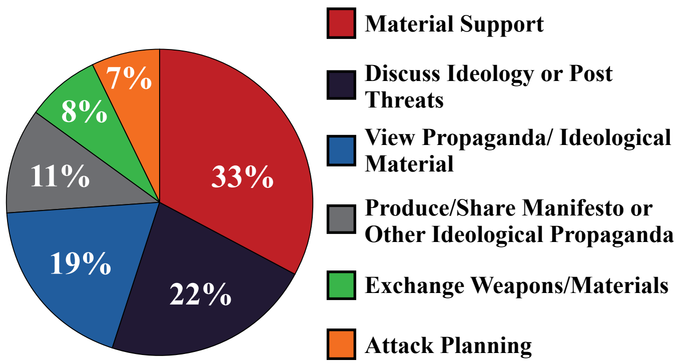


Domestic and Homegrown Violent Extremist Use of Social Media

Domestic Extremist Use of Social Media



HVE Use of Social Media



WRME Case Study

In November, Seann Pietila of Pickford, Michigan, pleaded guilty for making violent threats online. In June, Pietila allegedly used Instagram, Discord, and Pinterest to plan acts of violence, share neo-Nazi and antisemitic sentiments, and glorify past mass shooters. In a message to another user discussing his plan to attack a synagogue, he wrote, "I won't be taken alive I'll make sure of that. Remember Heil Hitler!" Pietila planned to livestream the attack online so it could be widely shared.

HVE Case Study

In July, federal authorities arrested Kamal Fataliev of Philadelphia, for lying to federal agents about his contact with ISIS sympathizers. Using an unidentified online chat platform, Fataliev uploaded more than 200 bomb-, poison-, and firearms-making guides to terror-related chat groups. He admitted that his social media profiles used ISIS imagery, such as the ISIS flag, so that other users could see his affiliation with the group. During interviews with authorities, Fataliev stated that he believed members of an online chat group were legitimate ISIS fighters who would use the information that he provided to create explosives.

Extremists Continue to Rely on Mainstream Platforms

Domestic extremists and HVEs continue to heavily rely on mainstream platforms for a variety of uses. Some platforms, such as X (formerly Twitter), have introduced enhanced or paid subscription models promising features like blue checkmarks and algorithmic boosts to help posts gain visibility and perceived credibility. These changes present an opportunity for those seeking an online space to share ideological material to large audiences. In February 2023, a WRME account with a subscription on X discussed the Great Replacement Theory in a post, which received 1.6 million views and was shared over 2,500 times. In October 2022, another WRME account shared to their Telegram channel, "Go on Twitter and let them know. Our time has come." Other mainstream platforms, such as YouTube and Instagram, have also seen increased engagement with extreme content on their sites. In November, an al-Qa'ida publication from November 2002 was widely recirculated across mainstream platforms, regardless of efforts to remove it. The Institute for Strategic Dialogue reported a 400 percent increase in YouTube searches related to the publication and increased Instagram algorithmic amplification. Extremist accounts capitalize on this increased interest and inconsistent content moderation to amplify their content into more mainstream spaces rather than the alternative platforms where they typically thrive.

Social Media Leveraged for Critical Infrastructure Attacks

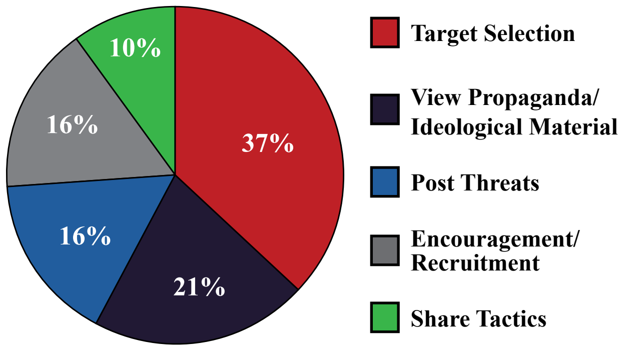
Domestic extremists will use social media and encrypted messaging platforms to share tactics, recruit and provide encouragement, and obtain guidance on target selection prior to selecting and attacking critical infrastructure. Between 2020 and 2023, there were 56 attacks, plots, and threats on critical infrastructure, and in 29 of those cases, domestic extremists used social media in their pre-operational activities.

In September, a five-step process on "how to kill a fed" circulated on 4chan, an anonymous online imageboard. The post encouraged viewers to lure police officers to their homes and attack them with firearms. In March, eco-fascist and white racially motivated extremist (WRME) channels shared an eco-extremist publication titled "Anti-Tech Quarterly," describing vulnerabilities across energy, communications, and cyber infrastructure. In June 2022, WRME members of "Terrorgram," a Telegram collective, began sharing a tactical document titled "Make it Count: A Guide for the 21st Century Accelerationist." This document called for attacks on infrastructure – namely the power grid, telecommunications systems, and pipelines – to bring about societal collapse.

In August, an unidentified user on Gab, an alternative social media platform, posted a list of individuals who work for specific critical infrastructure sectors, such as journalists and academics. The post encouraged followers "to go after" these targets as they have "poor security" when compared to larger facilities. Most followers agreed with the post, resharing it and further contributing to the list. In April, an unidentified subject posted on Telegram, offering monetary incentives to encourage attacks on communication and energy infrastructure. Users across several Telegram channels circulated the post and shared it with their followers.

In February 2023, federal authorities arrested two WRMEs, Sarah Clendaniel, of Catonsville, Maryland, and Brandon Russell, of Orlando, Florida, for plotting to attack several substations in the Baltimore area. Between June 2022 and February 2023, the pair used Telegram and other encrypted messaging platforms to plan attacks against electrical substations, noting the potential for a "cascading failure" if attacked. The two communicated their intent to "completely destroy [the] whole city." Russell and Clendaniel targeted the Baltimore area because of its five substations, which serve as major lifelines to other critical infrastructure sectors.

Social Media Usage, 2020-2023



This assessment evaluates trends and patterns of 29 domestic extremist attacks, plots, and threats targeting critical infrastructure. In cases where threat actors used social media for more than one pre-operational activity, the incident counted across multiple categories. This data only reflects open-source information related to critical infrastructure incidents nationally and may be subject to change.

Counterintelligence

Counterintelligence

The U.S. persistently confronts foreign intelligence threats emanating from nation-states such as China, Russia, and Iran. These adversaries aim to compromise our national and economic security to further their respective scientific, economic, and military development objectives. The spectrum of threats to the U.S. national security spans various actors, including nation-state actors equipped with advanced intelligence services and cyber programs, as well as nations with comparatively limited technical capabilities but potentially greater disruptive intent. In addition, the array of threats includes ideologically motivated hackers, profit-driven criminal enterprises, terrorist organizations, and internal actors.

In 2018, the New Jersey Office of Homeland Security and Preparedness (NJOHSP) created a counterintelligence program to anticipate, deter, and counter these threats as well as educate state equities on prevention techniques.

NJOHSP defines counterintelligence as activities designed to prevent or thwart an enemy or other foreign entity, such as nation-state actors, from spying, intelligence gathering, and sabotage.

The formation of a state-level Counterintelligence Unit (CIU) within NJOHSP is a necessary and proactive response to the rising tide of foreign threats. The CIU fills a critical gap in our State's security infrastructure, helping to ensure a safer and more secure New Jersey.

The creation of the Counterintelligence Unit provides many benefits for New Jersey, including:

- Increased security for the State's critical infrastructure
- Protection of the State's intellectual property and economic interests
- Mitigation of the impact of malicious foreign influence
- Strengthening of the State's democratic institutions

Detect

Deter

Disrupt

Identify the presence or existence of nefarious nation-state activities.

Discourage nation-state actors from conducting illegal operations

Interrupt and prosecute individuals or groups illegally operating in New Jersey

For more information about counterintelligence awareness, or to request a counterintelligence threat briefing, please contact notify@njohsp.gov.

Foreign Governments Target New Jersey for Economic and Military Advantages

Nation-state actors and individuals working at the behest of foreign governments are actively targeting industries throughout New Jersey to gain economic and military advantage over the U.S. Over the last five years, a diverse range of nation-state threat actors have targeted New Jersey through physical, cyber, and technical techniques that negatively impact private-and public-sector entities.

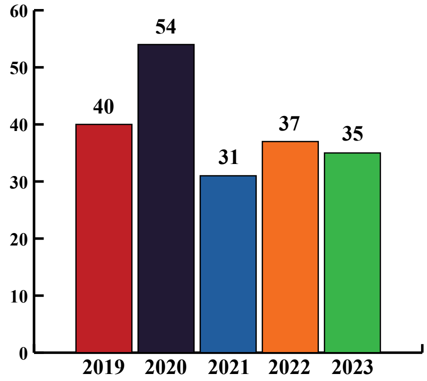
In December, a federal court sentenced Charles McGonigal, a former Special Agent in Charge of the FBI Counterintelligence Division in New York, to 50 months in prison and ordered him to pay a $40,000 fine for conspiring to violate the International Emergency Economic Powers Act (IEEPA) and to commit money laundering. In 2021, McGonigal agreed to provide “services” to a sanctioned Russian oligarch.

In October, federal authorities arrested and charged four individuals on two separate conspiracies to unlawfully export controlled, dual-use technologies to Russia following Russia’s invasion of Ukraine. In the first case, law enforcement arrested a New York resident and two Canadian nationals in connection with a “sophisticated global procurement scheme in which the defendants used two corporate entities registered in Brooklyn to unlawfully source and purchase millions of dollars’ worth of dual-use electronics on behalf of end-users in Russia, including companies affiliated with the Russian military.” In the other case, authorities charged a New York resident with an illegal exports scheme to procure dual-use electronic components for entities in Russia involved in the development and manufacture of drones for the Russian war effort in Ukraine.

In June, a federal jury convicted three defendants of acting and conspiring to act in the U.S. as illegal agents of the People’s Republic of China (PRC), without prior notification to the Attorney General. A court convicted Michael McMahon of Mahwah (Bergen County), a retired NYPD Sergeant, of acting as an illegal agent of the PRC, interstate stalking, and conspiracy to commit interstate stalking. The jury also convicted two additional defendants from New York of conspiracy to act as an illegal agent of the PRC, acting as an illegal agent of the PRC, conspiracy to commit interstate stalking, and interstate stalking.

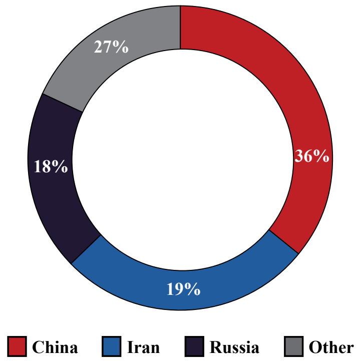
In May, the Department of Justice announced criminal charges in three cases in connection with the Disruptive Technology Strike Force, an interagency task force. Two of the cases in New York involve the disruption of alleged procurement networks created to help Russian military and intelligence services obtain sensitive technology in violation of U.S. laws. The third case involved a Chinese procurement network established to provide Iran with materials used in developing weapons of mass destruction (WMD) and ballistic missiles.

Federally Indicted Cases



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

Counterintelligence Cases by Country, 2019-2023



> “There is no doubt that the greatest long-term threat to our nation’s ideas, our economic security and our national security is that posed by the Chinese communist government. To be clear, that threat stems from the Chinese government, not the Chinese people themselves… the current Chinese regime will stop at nothing, steal what they can’t create, and silence the messages they don’t want to hear, all in an effort to surpass us as a global superpower and to shape a world order more friendly to their decidedly authoritarian regime.”
>
> FBI Director Christopher Wray on the China Threat, April 2023.

Insider Threat

Foreign actors will likely commit theft, cyber intrusions, and talent recruitment to steal intellectual property negatively impacting private-sector entities. Nation-state actors use trusted insiders (employees, researchers, and others), substantial financial investment, and other means to gain access to companies' valuable data. This can include the theft of proprietary data, critical technology and research; the compromise of networks and supply chain; the loss of competitive advantage or organizational reputation and unforeseen legal liabilities.

Insider Threat Indicators

Gathering Information

- Keeping information in unauthorized locations
- Attempting to access sensitive information without authorization
- Obtaining access to sensitive information inconsistent with present duty requirements

Information Transmittal

- Removing sensitive information
- Using unauthorized devices or methods to transmit or send information
- Discussing sensitive projects through non-secure methods

Unexplained Affluence

- Living a lifestyle inconsistent with known income
- Sudden purchases of high-value items or repayment of large debts
- Frequent personal travel beyond known income

Disgruntlement with Employer or U.S. Government

- Any statement that suggests conflicting loyalties that may affect handling of sensitive data
- Active attempt to encourage coworkers or others to violate laws or disrupt work operations
- Repeated statements that indicate an abnormal fascination with a strong desire to engage in espionage

Other Potential Indicators

- Behavior indicating concern that one is being investigated or watched
- Repeated or unrequired work outside of normal duty hours
- Part-time employment or outside activity which may create conflict of interest
- Attempts to conceal any activity of counterintelligence indicator(s)

Operational Security (OPSEC)

Safeguarding critical and sensitive information is essential to protect the success of an organization and its mission. Operational security (OPSEC) is a method of denying adversaries access to critical information.

Key Parts of OPSEC

Identify Critical Information. Critical information is factual data about an organization's intentions, capabilities, and activities that an adversary needs to plan and act effectively to degrade operational effectiveness or place the potential for organization success at risk.

Analyze Threats. Threat analysis consists of determining an adversary's ability to collect, process, analyze, and use information. The objective of threat analysis is to know as much as possible about each adversary and their ability to target an organization. It is especially important to tailor the adversary threat to the actual activity and determine what the adversary's capabilities are with regard to the specific operations of the activity or program.

Analyze Vulnerabilities. Adopt an adversarial view of the activity requiring protection. Identify weaknesses that an adversary can exploit as part of their collection capabilities.

Assess the Risks. Threats and vulnerabilities are compared to determine the potential risk posed by adversary intelligence collection activities targeting an activity, program, or organization.

Apply Countermeasures. Develop countermeasures to protect an organization's activity and eliminate the adversary threat.

Foreign Actors Targeting U.S. Residents Through Illegal Means

Through transnational repression, foreign actors are actively targeting their political opponents, dissidents, journalists, and others living in the U.S. to silence their activities and coerce compliance. Transnational repression can include stalking, harassment, hacking, physical violence, arrest or extradition requests to third-party countries, attempted kidnapping or forced return to a home country, threats, detainment of a target's family members overseas, freezing of financial assets, and online disinformation campaigns.

In November, federal authorities charged Indian national Nikhil Gupta in a murder-for-hire plot. According to court documents, Gupta, an Indian government employee, and his overseas-based co-conspirators directed a plot to assassinate an attorney and political activist who is a U.S. citizen of Indian origin residing in New York City. The alleged victim is a vocal critic of the Indian government and leads a U.S.-based organization that advocates for the secession of Punjab, a state in northern India that is home to a large population of Sikhs, an ethnoreligious minority group in India. The victim has publicly called for some or all of Punjab to secede from India and establish a Sikh sovereign state called Khalistan. The Indian government has banned the victim and the separatist organization from India.

Transnational repression is foreign government-backed transgression levied outside its borders to target, coerce, or otherwise harm U.S.-based individuals in violation of international norms, U.S. laws, and individuals' rights and freedoms.

In April, federal authorities charged two defendants in connection with opening and operating an illegal New York City-based police station for the Ministry of Public Security (MPS) of the PRC. The two subjects allegedly acted as agents of the PRC government and obstructed justice by destroying evidence of their communications with an MPS official. The defendants reportedly worked together to establish the first overseas police station in the U.S. on behalf of the MPS. The police station occupied a floor in an office building in Manhattan's Chinatown, but closed in the fall of 2022 after those operating it became aware of the FBI's investigation. MPS leveraged the illegal police station to monitor and intimidate dissidents and those critical of the PRC government.

In January 2023, federal authorities in New York unsealed murder-for-hire and money laundering charges against three members of an Eastern European criminal organization who authorities accused of plotting the murder of a U.S. citizen. The Iranian government targeted the victim for speaking out against the regime's human rights abuses. According to U.S. Attorney General Merrick Garland, "The Victim in this case was targeted for exercising the rights to which every American citizen is entitled. The Victim publicized the Iranian Government's human rights abuses; discriminatory treatment of women; suppression of democratic participation and expression; and use of arbitrary imprisonment, torture, and execution."

Anyone residing or visiting the U.S., including a U.S. territory, has freedom of speech protections, regardless of citizenship. To report any information potentially related to this matter, contact or refer to:

- The FBI Transnational Repression Website
- The FBI online at tips.fbi.gov
- Your local FBI field office
- 1-800-CALL-FBI (1-800-225-5324)
- Online Threat Intimidation Guide

Cybersecurity Threats

Executive Summary

The New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) assesses with high confidence that, in 2024, New Jersey's public and private institutions, critical infrastructure assets, and residents will continue to face an array of cyberattacks that are costly and operationally debilitating. These attacks will have the potential to adversely impact public health, the welfare and safety of our residents, the economy and public interests of the State, and national security.

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

This threat assessment highlights key trends, significant incidents, profiles of threat actors, systemic risks, and emerging technologies, providing actionable insights for enhancing the cybersecurity posture across New Jersey.

Key Points

- New Jersey faces an incessant and evolving threat landscape, characterized by cyberattacks that can be launched from anywhere in the world at any time of day or night.
- Public- and private-sector organizations are highly likely to be subjected to cyberattacks, requiring robust security measures and proactive threat mitigation.
- Nation-state actors, cybercrime syndicates, hacktivists, and others with diverse motivations and considerable technical capabilities present significant threats.
- Geopolitical unrest will influence the cyber threat landscape.
- Systemic cyber risk threatens widespread disruptions and cascading failures across sectors, requiring collaborative efforts to build resilience and enhance preparedness.
- The rapid evolution and adoption of emerging technologies, such as artificial intelligence, necessitates continuous adaptation and innovation in cybersecurity practices.

New Jersey's public- and private-sector institutions, as well as its residents, face a consistent and credible threat of cyberattacks from multiple types of threat actors with varying capabilities and motivations. Nation-state actors, such as China, Russia, Iran, and North Korea, have targeted American companies and infrastructure for espionage and potential disruption of critical systems. Transnational cybercrime syndicates, such as LockBit, Cl0P, and BlackCat/AlphV, continue to conduct financially motivated ransomware attacks on all manner of organizations, including hospitals, local governments, law enforcement agencies, large and small businesses, and educational institutions. In 2023, the NJCCIC documented more than 4,100 ransomware attacks worldwide that were publicly listed on the respective threat actors' leak sites and elsewhere. The ransomware victim lists contained **60** New Jersey public- and private-sector organizations, including CentraState Medical Center, Capital Health Hospital System, and Ardent Health Services/Hackensack Meridian Hospitals, the Camden County Prosecutor's Office, the Camden County Police Department, B&G Foods, Montclair Township, and Shore Regional School District.

Hacktivist groups, motivated by political, religious, and other causes and ideologies, have demonstrated their capability to cause outages as a result of highly disruptive distributed denial-of- service (DDoS) attacks and their ability to gain unauthorized access to systems which are used to manage energy and water systems. In 2023, KillNet, a hacktivist collective aligned with the Kremlin in Russia, carried out various DDoS attacks against public- and private-sector organizations as retribution for their respective countries' support of Ukraine. These DDoS attacks targeted websites and other online services provided by airports, state, and federal governments, and hospitals across the U.S., including AtlantiCare in New Jersey. KillNet is only one of numerous hacktivist groups that have launched cyberattacks against public- and private-sector entities in relation to both the Russia-Ukraine war and the Israel-HAMAS conflict.

The 2021 Colonial Pipeline ransomware attack disrupted fuel supplies across the Southeastern U.S. for days. The 2020 SolarWinds supply chain attack compromised thousands of public- and private-sector entities. In May 2023, a mass exploitation of a vulnerability in approximately 2,100 MOVEit file transfer servers worldwide resulted in the exfiltration of personal information of over 60 million individuals. According to reports submitted through the NJCCIC's data breach reporting system, the compromise of MOVEit systems, which are maintained by 202 organizations throughout the U.S., resulted in the exfiltration of more than 1 million New Jersey residents' sensitive personally identifiable information (PII). In October 2023, a vulnerability in the remote access appliance software of Citrix NetScaler products, dubbed Citrix Bleed, allowed threat actors to mass exploit the networks of companies and organizations around the world. The impact of this mass exploitation closed Australia's shipping ports for days, resulted in the breach of sensitive PII of approximately 36 million Comcast customers, and forced hospitals in New Jersey and across the U.S. to divert patients from their emergency rooms, postpone surgeries, and use paper-based processes, thereby slowing patient care.

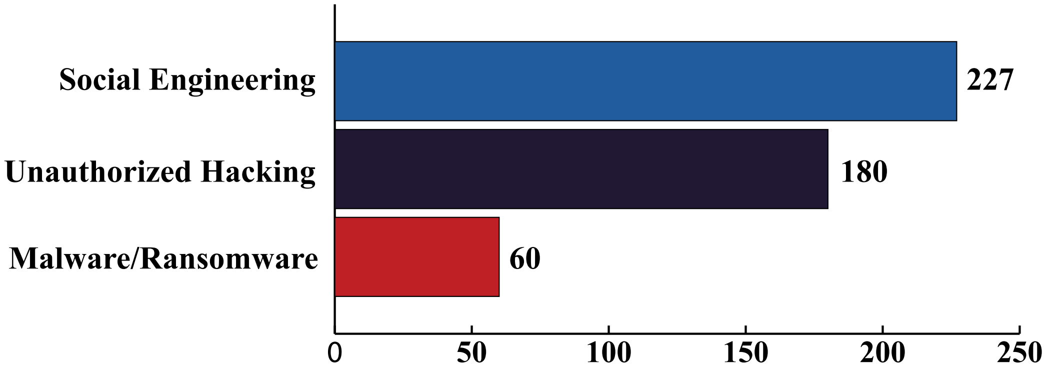
These and other incidents highlight how, in a hyperconnected world, cyberattacks are not constrained by geographic borders, and such attacks can result in cascading impacts across industries, regions, and the world. The nature and consequences of such cyberattacks provide an indication of the potential cybersecurity challenges in which New Jersey and the nation will face going forward.

Incident Reporting

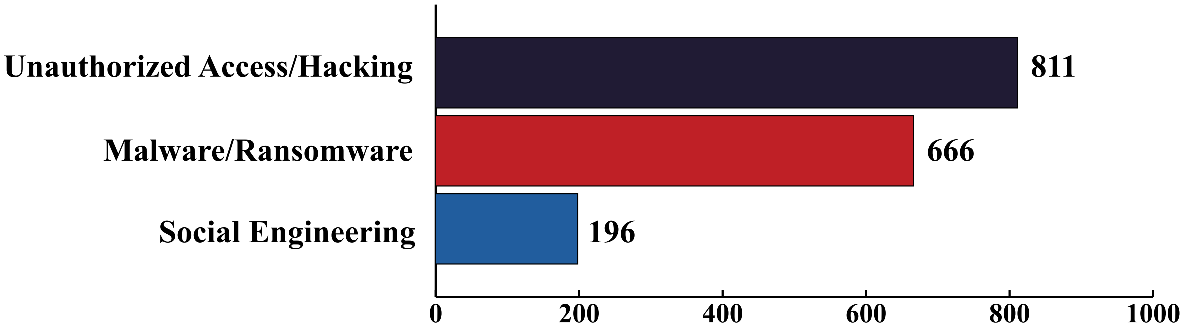
In New Jersey, not all cyberattacks are publicly disclosed or reported to the NJCCIC. Therefore, a complete accounting of cybersecurity incidents, impacting New Jersey-based organizations and individuals, is not feasible. Overall, the number of cyber incidents reported to the NJCCIC from all victims remains virtually unchanged in 2023 (**542**), as compared to 2022 (**531**) and 2021 (**559**). On March 13, 2023, Gov. Phil Murphy signed into law P.L. 2023, c.19 (C.52-17B-193.2) requiring public agencies and government contractors that provide services to public agencies to report cybersecurity incidents to the NJCCIC. As a result, the NJCCIC has seen a **41 percent increase** in reported incidents (**163**) from public agencies and government contractors in 2023. By submitting incident reports, the NJCCIC can offer assistance to the affected entity to help respond to and recover from the incident. Intelligence gleaned from submitted incident reports also helps the NJCCIC to identify novel and trending attack vectors, to develop and share best practices for defending against such cyberattacks, and to help reduce cyber risk throughout the state.

In 2023, the three most prevalent incident types reported to the NJCCIC included: **Social Engineering** (**227**), via phishing emails, text messages, and voice calls; **Unauthorized Access/Hacking** (**180**); and **Malware/ Ransomware Attacks** (**60**). According to reports submitted through the NJCCIC's data breach reporting system, the three most prevalent causes of data breaches reported in 2023 were **Unauthorized Access/Hacking** (**811**), **Malware/Ransomware** (**666**), and **Social Engineering** (**196**).

Top 3 Incident Types Reported to NJCCIC

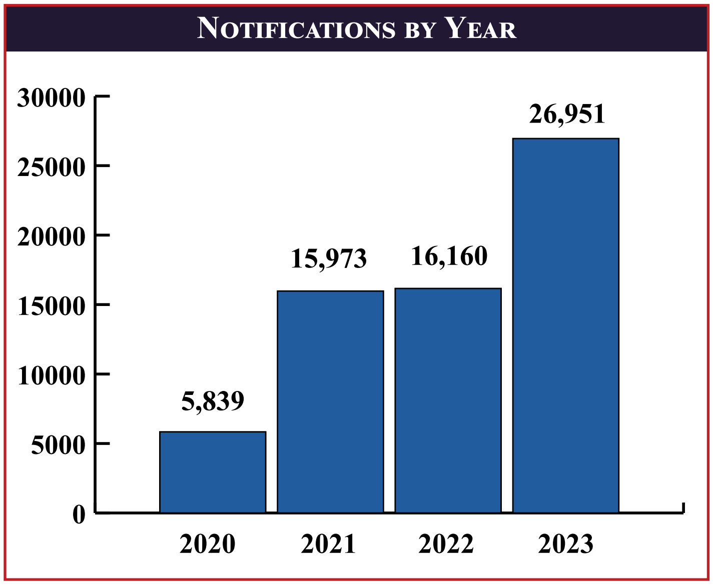


Top 3 Data Breach Causes



Compromised Login Credentials as an Attack Vector

According to the 2023 Verizon Data Breach Report, up to **80 percent of all breaches**, including unauthorized access and human operated ransomware attacks, are the result of stolen or otherwise compromised login credentials. To combat such attacks, the NJCCIC proactively searches for and harvests the compromised credentials (email addresses/passwords) of New Jersey public sector and select critical infrastructure personnel that are published on dark web, paste sites, and other internet sites. Published email addresses in scope are limited to work and school accounts. In 2023, the NJCCIC made **26,951 notifications** to affected New Jersey organizations of their compromised employee and/or student login credentials as well as instructions for mitigating the risk of their potential misuse. Compromised login credentials are a favored method for threat actors to gain unauthorized access to networks, often without detection, by appearing as legitimate logins. Various reports estimate there are over 6.7 billion sets of compromised credentials 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 2024.



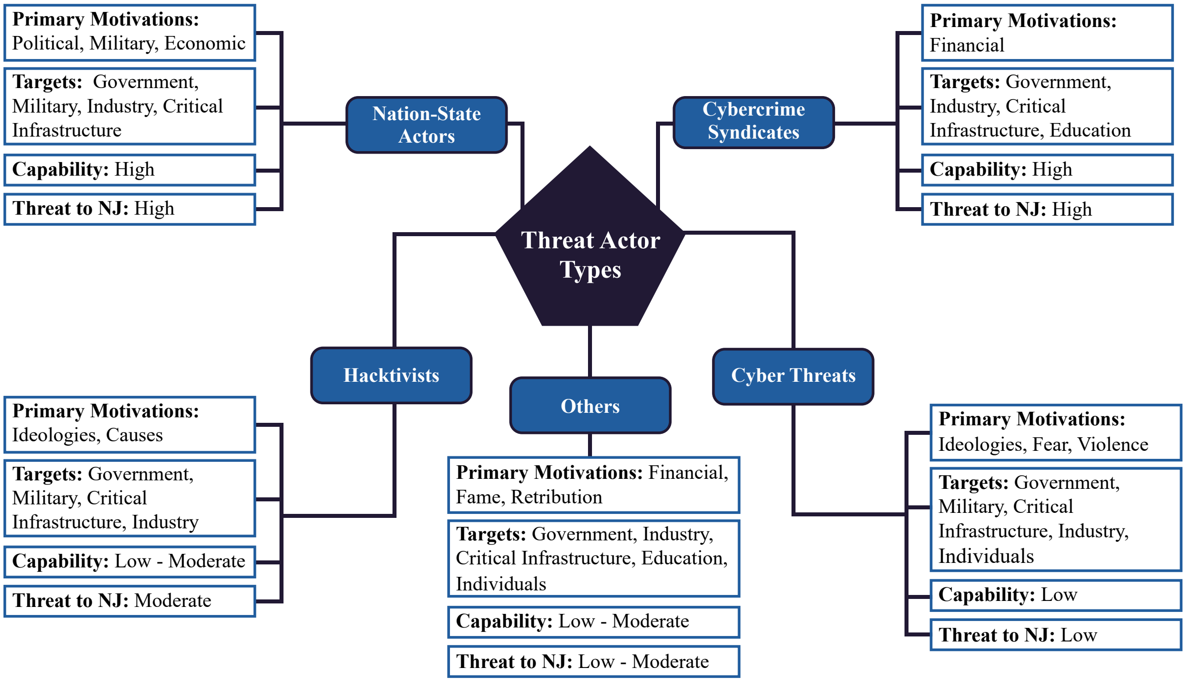
Notifications by Year

Sector	Count
Education Sector	24,623
Water Sector	621
State Government	603
Healthcare Sector	550
Municipal Government	279
County Government	187
Law Enforcement	88
Total	**26,951**

Figure 1 - Compromised credentials notifications made by the NJCCIC per year and by sector for 2023.

Threat Actors

Threat actor is a broad term used to describe any individual or group that conducts malicious cyber acts against a person or an organization. They include nation-state threat actors, cybercrime syndicates, hacktivists, cyber terrorists, and other threat actors. These threat actors are responsible for the majority of significant cyberattacks and pose the greatest threat to New Jersey and the nation. While each group has some unique characteristics, it is often difficult to discern the true alignment of cybercrime syndicates, hacktivists, and cyber terrorists, as they may covertly act on behalf of or in support of nation-state interests despite appearances of independence.



Threat Actor Types

Nation-State Actors

Primary Motivations: Political, Military, Economic

Targets: Government, Military, Industry, Critical Infrastructure

Capability: High

Threat to NJ: High

Cybercrime Syndicates

Primary Motivations: Financial

Targets: Government, Industry, Critical Infrastructure, Education

Capability: High

Threat to NJ: High

Hacktivists

Primary Motivations: Ideologies, Causes

Targets: Government, Military, Critical Infrastructure, Industry

Capability: Low - Moderate

Threat to NJ: Moderate

Others

Primary Motivations: Financial, Fame, Retribution

Targets: Government, Industry, Critical Infrastructure, Education, Individuals

Capability: Low - Moderate

Threat to NJ: Low - Moderate

Cyber Threats

Primary Motivations: Ideologies, Fear, Violence

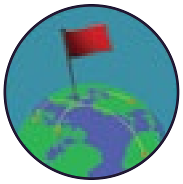
Targets: Government, Military, Critical Infrastructure, Industry, Individuals

Capability: Low

Threat to NJ: Low

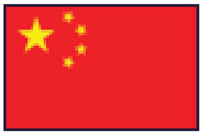
Figure 2 – High-level overview of major cyber threat actor types.

Major Threat Actor Groups



Nation-State Threat Actors

Nation-state actors, also sometimes interchangeably referred to as state-sponsored actors, are threat groups who work in support of, or directly for, a government body/state apparatus, such as an intelligence service to further their geopolitical, military, or economic objectives through cyber operations. They are generally well resourced and utilize advanced tools, techniques, and procedures (TTPs) to engage in stealthy and long-term operations at the direction or on behalf of the nation state. China, Russia, Iran, and North Korea are generally considered the four primary adversarial nation-state actors that continue to present the greatest and most persistent threats to New Jersey and the nation. They are all adept at using cyber operations to further their strategic goals through various techniques, including espionage against government and industry targets, prepositioning on critical infrastructure networks for future operations, building networks of compromised devices to enable malicious activity, executing highly disruptive cyberattacks on infrastructure and businesses, and engaging in information operations to spread propaganda and disinformation.



China

China represents one of the most capable and persistent nation-state cyber threats. The Ministry of State Security (MSS) and the People's Liberation Army's Strategic Support Force (PLASSF) lead China's cyber operations to conduct global cyber espionage operations and steal intellectual property to support China's economic and military modernization. Key targets include political, economic, military, and critical infrastructure networks. China-linked groups have become known for sophisticated, stealthy intrusions designed to silently gather intelligence for the long term.

In July 2023, Volt Typhoon, a threat actor group affiliated with the PLASSF, was reported to have compromised nearly two dozen critical infrastructure organizations, including those specializing in communications, manufacturing, utility, transportation, construction, maritime, government, information technology, and education, across the U.S. To evade detection, Volt Typhoon employed stealth techniques, such as leveraging compromised Small-Office Home-Office (SOHO) devices to obfuscate the origin of their activity and using Living Off the Land (LOTL) tools for discovery and lateral movement. Its activities have been linked to the theft of classified information and intellectual property from organizations in the targeted industries. While no known destructive operations have been carried out by Volt Typhoon, it is still capable of remaining undetected and prepositioned on victim networks.

Other notable state-sponsored threat actor groups affiliated with China's government, military, and intelligence services include Hafnium, Storm-0588, and APT-41. Hafnium is responsible for exploiting previously unknown Microsoft Exchange Server vulnerabilities in early 2021 to compromise tens of thousands of organizations globally, including at least three local governments in New Jersey. In July 2023, Microsoft and U.S. officials reported that the Chinese State-linked threat actor Storm-0558 had gained unauthorized access to the Microsoft365 email accounts at 25 federal government organizations, including the U.S. Department of Commerce and the U.S. Department of State. At least 60,000 emails were exfiltrated during the attack. APT-41 has been conducting both state-sponsored targeted intrusions that often align with Chinese Communist Party (CCP) objectives as well as criminally focused operations since at least 2014. In 2020, the U.S. Department of Justice (DOJ) indicted seven individuals linked to APT-41 for their roles in hacking, identity theft, money laundering, and wire fraud crimes. More recently, APT-41 has been linked to the theft of more than $20 million in U.S. COVID-19 Economic Relief benefits. These four groups represent only a small fraction of China's state-sponsored cyber threat apparatus. As China continues to use these groups to support its long term economic and military goals, they are a highly capable and well-resourced advanced persistent threat (APT) to New Jersey in 2024 and beyond.

Russia

Russia represents one of the most formidable and aggressive nation-state cyber threats. Russian cyber operations are primarily conducted by intelligence services, such as the Federal Security Service of the Russian Federation (FSB), the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU), and the Foreign Intelligence Service of the Russian Federation (SVR), often targeting government, military, diplomatic, and other organizations and businesses worldwide for intelligence that benefits Russia's foreign policy and military decision-making. Russian state-sponsored cyber actors are adept at developing custom malware and exploiting previously unknown vulnerabilities in software to target government, military, and private sector networks globally.

Over the past several years, a number of debilitating and destructive cyberattacks have been attributed to the GRU. In December 2015, GRU operatives, referred to as Sandworm, launched cyberattacks against Ukraine's power grid, resulting in power outages for hundreds of thousands in the Kyiv region. The malware used to disable the power grid also wiped and destroyed files on infected computer systems. In 2016, the GRU refined its malware and automated its cyberattacks against Ukraine's power grid causing more power outages. In 2017, the GRU inserted malware into an accounting software update which resulted in the most damaging cyberattack in history. While the malware was intended to target and cripple businesses operating in Ukraine, its destructive nature spread worldwide, impacting Merck and the Port Newark Container Terminal in New Jersey. This cyberattack is known as NotPetya and resulted in more than $10 billion in damages worldwide, including over $1.4 billion in New Jersey alone. As with the power grid attack in Ukraine, the malware used in NotPetya infected and wiped computer systems. In 2020, U.S. DOJ indicted six GRU officers for their roles in the Ukraine power grid and NotPetya attacks, as well as several other cyberattacks.

In late 2020, the cybersecurity firm Mandiant discovered it had been the victim of a sophisticated espionage-focused software supply chain attack that was later attributed to the Russian SVR group, APT-29 (aka Cozy Bear), which leveraged trojanized SolarWinds Orion network management software to breach numerous U.S. government agencies, critical infrastructure entities, and major technology companies. These victims included the Department of Defense, the Department of Treasury, the Department of Homeland Security (DHS), Microsoft, Cisco, Palo Alto Networks, and many others. Several New Jersey organizations also installed the trojanized software on its networks, although there are no reports or evidence that it was used by the SVR to conduct any further illicit activities against these organizations. The trojanized software that remained undetected for almost 14 months demonstrates the capabilities of Russian state-sponsored threat actors to stealthily infiltrate their targets' networks. The SolarWinds incident also demonstrates that APT groups will exploit trusted technology supply chains and service providers to obscure attribution and enable widespread access. The SolarWinds hack exemplifies systemic risks that will continue to threaten New Jersey public and private sector organizations as sophisticated adversaries target weakly secured infrastructure and software supply chains.

Furthermore, as evidenced during the 2016-2020 U.S. presidential campaign cycles, Russian state-sponsored threat groups present a threat to candidates' campaigns, national campaign committees, and state and local election infrastructure. With the upcoming 2024 U.S. presidential election, New Jersey anticipates the targeting of its election infrastructure and widespread misinformation campaigns by Russian operatives.

Major Threat Actor Groups

Iran

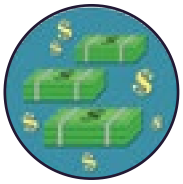
Iran poses a significant cyber threat to New Jersey as evidenced by recent indictments and global cyberattacks. In September 2022, the U.S. Attorney's Office for the District of New Jersey charged Iran with engaging in computer intrusions and ransomware-style extortion against U.S. critical infrastructure providers, small businesses, government agencies, nonprofit programs, and educational and religious institutions. Their victims also included one municipality and one business in New Jersey. The indictment revealed that the defendants' hacking campaign exploited known vulnerabilities in network device software, causing damages and losses to the victims.

In November 2023, a series of cyberattacks attributed to CyberAv3ngers, an Iranian-backed APT group, targeted water and wastewater utilities nationwide. In these incidents, the threat actors compromised Unitronics programmable logic controllers (PLCs) used mainly in the water and wastewater sector but also implemented in other industries, including energy, food and agriculture, and healthcare and public health. CyberAv3ngers claimed responsibility for over a dozen cyberattacks launched since October 30, 2023, stating that they targeted Unitronics as it is Israeli-made and "Every equipment 'made in Israel' is CyberAv3ngers legal target." These incidents are evidence of the active and ongoing threat posed by Iran in the cyber domain to New Jersey's critical infrastructure and businesses.

North Korea

North Korea is commonly named as one of the top cyber adversaries to the U.S.; however, they often operate much differently than cyber adversaries such as China, Russia, and Iran. North Korea leverages its cyber capabilities for financial theft and disruption to generate revenue and retaliate against adversaries. In 2023, the theft of over $600 million in cryptocurrency has been attributed to North Korean state-sponsored threat actors.

North Korean intelligence bureaus, such as the Reconnaissance General Bureau (RGB), conduct the nation's cyber operations. Prominent North Korean threat groups, including the Lazarus Group and APT-38, carry out cyber operations worldwide. In 2014, Lazarus Group hacked Sony Pictures in retaliation for releasing the film The Interview, wiping data and leaking internal documents. The film is a political satire in which the CIA plots to use two U.S. journalists to assassinate North Korean leader Kim Jon Un. In 2016, APT-38 stole $81 million from the Bank of Bangladesh. In 2018, the U.S. DOJ attributed the May 2017 WannaCry ransomware attack, which infected over 300,000 computers in 150 countries, to North Korea. Over 70,000 computers in hospitals operated by the National Health Services in the United Kingdom were encrypted as a result of the WannaCry attack, thus impacting hospital operations and patient care throughout England and Scotland. Additionally, the WannaCry malware spread to and impacted numerous computer systems in New Jersey. These examples underscore the ongoing and evolving cyber threats posed by North Korea. Its ability to target healthcare and financial entities and launch debilitating and costly cyberattacks, such as the Sony Picture hack and WannaCry, makes North Korea a threat to New Jersey organizations in these sectors and beyond in 2024.



Cybercrime Syndicates

Cybercrime syndicates are sophisticated criminal organizations which leverage digital technologies to carry out illegal activities, primarily for financial gain. These activities include ransomware attacks, financial fraud, intellectual property theft, identity theft, and the sale of illegal goods and services on the dark web. These syndicates are often characterized by their hierarchical and compartmentalized structure and are often organized as a typical business with clear divisions of labor among members who may possess specialized skills in hacking, social engineering, money laundering, and other cybercrime techniques. They continually adapt their tactics to avoid detection, employing encryption, anonymizing tools, and other methods. The global nature of these syndicates poses significant challenges to law enforcement, often operating in jurisdictions with weak cybersecurity laws, limited resources for cybercrime investigations, and, in some cases, implicit or explicit permission of authorities. Even when law enforcement successfully shuts down an operation, syndicates are quick to relaunch them, while also rebranding under another name. Notable ransomware groups (and impacted victims) over the past several years include LockBit (Capital Health), BlackCat/AlphV (Caesars and MGM), Darkside (Colonial Pipeline), Conti (East Windsor), etc. The table to the right lists the top 10 ransomware types based on the number of impacted victims in 2023. In February 2022, the Conti ransomware group pledged its full support to Russian President Vladimir Putin and the Kremlin, thus further blurring the lines between state-sponsored and criminal activities.

Ransomware Type	# Victims
LockBit	1042
BlackCat/AlphV	458
CL0P	367
Black Basta	323
Play	322
8Base	250
Cactus	249
Akira	244
BianLian	243
Medusa	144

Table 1: Top 10 publicly disclosed ransomware types employed in attacks in 2023.

Hacktivists

Hacktivist groups use hacking techniques to promote social or political agendas and ideologies. They believe they can affect change and feel justified in targeting individuals, organizations, or government agencies in support of their beliefs and allegiances. Over the past two years, as a result of the Russia-Ukraine war and Israel-HAMAS conflict, multiple hacktivist groups have emerged targeting the infrastructure of their side's adversaries as well as those adversaries' allies.

For example, KillNet, a collective of members and volunteers who support Russian geopolitical ideology, began operations around March 2022 in support of Russia's invasion of Ukraine. The group has since conducted numerous DDoS attacks targeting government institutions and private companies directly and indirectly supporting Ukraine's war efforts. In addition, KillNet has also targeted the U.S. healthcare and public health sector with DDoS attacks, including New Jersey-based AtlantiCare Health System and the websites of New York and Philadelphia airports. In addition to KillNet, many other hacktivist groups have carried out cyberattacks in support of Russia's war efforts, including NoName057(16), Usersec, and Anonymous Sudan.

Since October 7, 2023, pro-HAMAS hacktivist groups, some affiliated with HAMAS, Hizballah, Iran, and other Palestinian groups, have launched many DDoS attacks against entities in Israel, as well as government and private sector organizations around the world that support Israel. As with the DDoS attacks launched by Russian hacktivists, their impacts last for only a brief period of time – hours to days – before the targeted sites recover. Beyond just DDoS attacks, these hacktivist groups have also carried out more nefarious attacks, such as hacking industrial controls systems of energy and water providers; exfiltrating and leaking sensitive information of government, healthcare, and military targets; and infecting targeted systems with wiper malware, resulting in debilitating operational impacts and significant financial losses for their victims.

As with cybercrime syndicates, such as Conti, the role and intentions of hacktivist groups are sometimes blurred as their activities may also be state-supported and sponsored. While the DDoS attacks initially launched were simply a nuisance to their targets, they have improved their tradecraft and capabilities over time and now pose a more significant threat.

Cyber Terrorists

Cyberterrorists, like hacktivists, use cyberattacks to advance their ideological agendas. Some cyber terrorists are nation-state actors; others act on their own or on behalf of a non-government group. To date, traditional foreign and domestic terrorist groups that use violence to achieve their goals have not demonstrated the advanced capabilities necessary to carry out significant cyberattacks. However, some of the hacktivist groups, who claim to be carrying out cyberattacks in support of their ideologies and causes, may also be members of and proxies for terrorist groups.

Other Threat Actors

Beyond the groups listed above, there are other loosely organized threat actor groups, such as Lapsus$, and other unaffiliated individuals that pose significant threats. Lapsus$, which was active in 2022 and 2023, was comprised of mostly teenagers from the United Kingdom, Brazil, and elsewhere. Lapsus$ members were responsible for hacking into some of the most cybersecure and valuable companies in the world, including Microsoft, Nvidia, Samsung, LG, and Uber. In the summer of 2023, British authorities arrested several members of the group who have recently been convicted for their crimes. Other members of Lapsus$ remain free. Lapsus$ often used social engineering and recruited insiders to help carry out its attacks, highlighting that initial access into otherwise secure networks may be accomplished via people and process vulnerabilities instead of technical vulnerabilities.

Lapsus$'s exploits demonstrated that nearly anyone with some technical and people skills, an internet connection, time, and motivation can successfully carry out attacks, even against targets that are very secure. Therefore, these loosely formed and ephemeral groups and unaffiliated individuals, similar to the other major threat actor groups, also pose threats to New Jersey's residents and public and private institutions.

Geopolitics and Their Impact on the Threat Landscape

Geopolitical conflicts and events across the globe pose various levels of threats to New Jersey in 2024. These conflicts, including the ongoing Russia-Ukraine war and the Israel-HAMAS conflict, have already led to targeted cyberattacks against critical infrastructure, businesses, and government entities in New Jersey and more broadly across the U.S. Also, geopolitical tensions elsewhere have the potential to trigger cyberattacks by nation-state actors, hacktivists, cyber terrorists, and others far beyond their physical boundaries. The 2024 U.S. presidential election is another triggering event that poses the threat of cyberattacks and malign foreign influence campaigns from around the globe aimed at disrupting the electoral process and further exacerbating social discord in the state and the country.

Russia-Ukraine War and its Impact on New Jersey

Since February 2022, when Russia invaded Ukraine, public- and private-sector organizations in western countries providing support for Ukraine have been the target of cyberattacks, primarily from Russian-aligned hacktivist groups. These groups, such as KillNet, NoName057(16), and Anonymous Sudan, have all carried out attacks against U.S. infrastructure. KillNet has been particularly active, primarily conducting large scale DDoS attacks against critical infrastructure targets, including hospitals across the country and in New Jersey. Due to Russia's sophisticated cyber capabilities and history of state-sponsored cyberattacks, the nation state and its proxies are seen as a significant threat to New Jersey's public- and private-sector cyber infrastructure.

Israel-Hamas Conflict and its Impact on New Jersey

The Israel-HAMAS conflict has raised concerns about cyberattacks, as both sides have engaged in cyberattacks in the past, and the potential for escalation in the cyber domain remains high. New Jersey, with its large Jewish and Muslim populations, is a potential target of cyberattacks linked to the conflict. Almost immediately after HAMAS' October 7 attack on Israel, various hacktivist groups began conducting cyberattacks against Israeli and western entities in support of HAMAS and Gaza.

Taiwan Strait Crisis

Rising tensions in the region may introduce risks of cyberattacks emanating from state-sponsored actors and hacktivists in China targeting western interests and infrastructure. New Jersey's efforts to forge closer economic and cultural ties with Taiwan may act as an aggravating factor or trigger for such attacks against the state's public- and private-sector organizations.

2024 US Presidential Election

Leading up to the 2016 and 2020 presidential elections, nation-state actors and their proxies conducted targeted cyberattacks against states' election infrastructure across the country. In addition, these threat actors carried out cyber-enabled mis-, dis-, and mal-information campaigns using social media platforms, email services, botnets, and troll farms. The campaigns promoted the threat actors' own political and national interests, attempting to coerce and sway U.S. voters, sow social discord, and erode trust in the electoral process.

2016 Elections - Russian Hacking of States' Elections Systems

In July 2016, Russian state-sponsored hackers exploited a web application vulnerability in the Illinois State Board of Elections website to illegally access sensitive personal information, including names, addresses, Social Security numbers, and drivers' license numbers of approximately 500,000 Illinois voters. The breach forced the board to shut down the voter registration system for 10 days to investigate the attack. While no evidence of voter data manipulation was found, the incident raised concerns about the vulnerability of election systems to cyberattacks.

The Illinois database breach was part of a broader Russian campaign targeting election infrastructure across multiple states that aimed to undermine confidence in the U.S. election process. According to a Joint Intelligence Bulletin and a Joint Analysis Report published by DHS and the FBI, the election infrastructure in all 50 states was researched by Russian government threat actors leading up to the 2016 presidential election. The research activity was aimed at identifying vulnerabilities and gaining access that could be exploited to undermine the election. Furthermore, Russian actors launched cyberattacks against at least 21 state voter registration and voter information systems, excluding New Jersey.

2020 Elections - Iranian Hacking and Voter Intimidation Campaigns

In November 2021, the U.S. Attorney's Office for the District of Columbia indicted three Iranian hackers—Seyyed Mohammad, Hosein Musa Kazemi and Sajjad Kashian—for attempting to compromise the voter registration systems of 11 states and accessing confidential voter data from at least one state. In addition, posing as members of the Proud Boys, Kazemi and Kashian sent threatening messages to tens of thousands of voters in battleground states, intending to intimidate and influence voters, undermine voter confidence, and sow discord in connection with the 2020 U.S. presidential election.

2023 New Jersey State Elections Infrastructure Threat Activity

The NJCCIC, in partnership with the New Jersey Department of State and its Division of Elections, implements various cybersecurity protections to safeguard the state's election infrastructure from cyberattacks. In 2023, the NJCCIC's defensive tools, technologies, and services detected and blocked over 105,000 indiscriminate and targeted attacks against the state's elections infrastructure. These included phishing and malware laden emails, as well as web application, credential stuffing, and other infrastructure attacks. The NJCCIC expects to see more attempted attacks against the state's election infrastructure in 2024.

The rapid evolution and adoption of emerging technologies, such as AI, presents both unprecedented opportunities and complex challenges, significantly impacting the cybersecurity landscape in 2024. The NJCCIC assesses that in the near-term, threat actors will exploit generative AI to produce highly convincing and personalized phishing content at scale, increasing the effectiveness of these cyberattacks. Deepfakes powered by generative AI enable the fabrication of realistic yet entirely falsified audio and video content. Threat actors are already using deepfakes in sophisticated impersonation schemes for fraud and disinformation campaigns. The distribution of deepfake multimedia content on social media and other online networks will likely be used by adversaries to sway opinions; sow unrest; undermine political candidates and their campaigns, thus threatening the integrity of the election process; and damage the reputations of governments, organizations, and individuals. There is already evidence that threat actors are using AI to develop malware and leverage AI to discover vulnerabilities and optimize targeting efficiency. While these use cases are in their infancy, it is highly likely that over time, AI will be used to amplify the capabilities of threat actors and the potential harms they can cause.

While AI brings immense societal benefits, unchecked proliferation also enables adversaries to weaponize these technologies against vulnerable targets at scale. AI and machine learning in critical systems introduce new attack surfaces ripe for exploitation. Adversarial techniques, such as data poisoning or evasion attacks, can manipulate AI models to misclassify malicious inputs or generate content that bypasses defenses. Autonomous vehicles, drones, robotics, and operational technologies in utility and manufacturing industries relying on AI for decision-making could be compromised to cause kinetic damage. As with any new and rapidly developing technology, there are many vulnerabilities in AI that have yet to be identified and addressed. For these reasons, governments and industry need to proactively implement and enforce strong AI governance models and risk management frameworks to effectively manage these risks.

Systemic Cyber Risk

In the current hyperconnected environment, a seemingly isolated system failure or compromise of an individual system can have cascading affects well beyond the initially affected system. Key systemic risks created by insecure software platforms, lack of visibility into third-party networks, and fragile supply chains create attack vectors for threat actors to compromise systems and cause cascading effects. As highlighted by the NotPetya, SolarWinds, MOVEit, and Citrix Bleed cyberattacks, such incidents have great impacts affecting societies, governments, industries, and individuals worldwide. In each of these instances, New Jersey organizations and individuals were adversely impacted. In another instance in which systemic risk figured prominently, a vulnerability discovered in December 2021 that allowed remote code execution via log messages due to improper input validation in the popular Java logging library, Log4j left hundreds of thousands of enterprises exposed until patched. This vulnerability was cited as a cause for the ransomware attack on one county in New Jersey. The systemic implications of cyberattacks on the critical infrastructure sector is highlighted by the 2021 Colonial Pipeline ransomware attack which disrupted the fuel supply throughout the Southeastern U.S.

Systemic risk is exacerbated by the proliferation and resultant dependencies on information technology throughout all facets of society, which is expected to continue for the foreseeable future. The sustained integration of embedded and networked technologies into physical devices used by governments, organizations, and individuals will highlight vulnerabilities that are prone to exploitation as a result of malicious activity, malfunction, human error, and acts of nature. This proliferation also creates an expanding attack surface which provides current and future opportunities for threat actors.

Conclusion of Cybersecurity Threats

Based on an analysis of cyberattack trends and emerging threats; the motivations, capabilities, and targeting by various threat actor types; geopolitical issues; and systemic cyber risks, the NJCCIC assesses with high confidence that in 2024, New Jersey's public and private sectors, critical infrastructure assets, and residents will continue to face an array of cyberattacks that are costly and operationally debilitating. These attacks will have the potential to adversely impact public health, the welfare and safety of our residents, the economy and public interests of the state, and national security.

It is unrealistic to expect any one person or organization to defend against nation-state actors, criminal syndicates, hacktivists, cyber terrorists, and other threat actor groups who can launch attacks from anywhere in the world at any time of day or night. Effectively managing cyber risk requires a proactive and collaborative approach. Public- and private-sector organizations at the federal, state, and local levels, as well as businesses large and small, must collaborate by sharing threat intelligence, implementing robust cybersecurity standards, and fostering a culture of vigilance.

NJ Office of Homeland Security and Preparedness

Resources

New Jersey Statewide Threat Assessment Team (NJ STAT)

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

The NJ STAT Steering Committee includes members from:

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

The NJ STAT provides alternative avenues for individuals who exhibit concerning behaviors and could be on the pathway to violence. It leverages existing partnerships at the local and county levels, including existing Counter-Threat Coordinator (CTC) programs, to establish multi-disciplinary county threat assessment teams (CTATs). Integral to the long-term success of the CTATs is the incorporation of partnerships across all levels of county government including non-traditional partners, such as mental health professionals, to establish an effective team.

The NJ STAT leverages existing platforms, such as the New Jersey Suspicious Activity Reporting System (NJSARS), to further support CTAT development. The NJSARS will remain the central data collection point for all information related to suspicious or criminal activity potentially related to terrorism and threatened acts of violence to both hard and soft targets as mandated by the update to New Jersey Attorney General Directive 2016-7. NJSARS is one of the primary referral mechanisms for behavioral threat-related cases supported by NJ STAT. From 2019 to 2023, a review of the NJSARS revealed a sharp increase in the number of school- and community-based threats which required a multidisciplinary response and management process.

All NJ STAT reports are reviewed and assessed for mobilization to violence indicators. Individuals who are identified with behavioral threat markers and have the potential to become targeted violence actors will be further evaluated.

NJ STAT Success Stories:

- ★ In January 2023, two high school students planned to kidnap and kill another classmate. Local law enforcement discovered the plot after one of the students made an online threat directed at the classmate. Through close coordination with the local police, school district, and the Monmouth County Prosecutor's Office, the NJ STAT team determined that one of the students had a previous relationship with the victim and still held a grievance against them. A consent to search of the suspect's room revealed weapons, blueprints, and materials related to white racially motivated extremism. Through coordination with the multi-agency/multi-disciplinary team, both persons of concern were criminally charged and provided appropriate treatment interventions.
- ★ In April, a juvenile in Bergen County created a social media account referencing the May 2022 Uvalde, Texas, school shooting that left 21 killed. The juvenile used the shooter's name for the account and posted comments related to the victims. The NJ STAT team facilitated conversations with the school and family, after the juvenile exhibited homicidal and suicidal ideations, to ensure this individual received the appropriate treatment interventions.

Interfaith Advisory Council

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

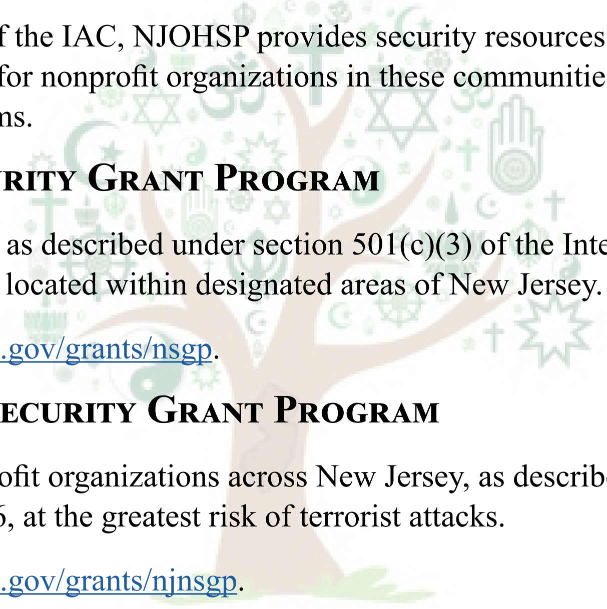
The IAC, led by the New Jersey Office of Homeland Security and Preparedness (NJOHSP), allows NJOHSP and State leadership to maintain an ongoing dialogue with all faith-based groups, across all 21 counties in New Jersey, wishing to participate. The Director of NJOHSP chairs the council.

Quick Facts

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

Learn more about the IAC at njohsp.gov/interfaith.

Community Resources



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

Federal Nonprofit Security Grant Program

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

For more information, visit njohsp.gov/grants/nsgp.

New Jersey Nonprofit Security Grant Program

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

For more information, visit njohsp.gov/grants/njnsgp.

New Jersey Shield Program

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

For member eligibility individuals must be:

- 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/newjerseyshield.

New Jersey Cybersecurity and Communications Integration Cell

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

Information Sharing

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

Cyber Threat Analysis

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

Incident Reporting

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

NJCCIC Membership

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

NJCCIC Cybersecurity Incident Reporting System

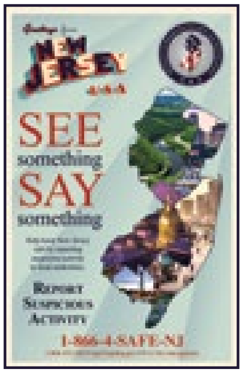
The NJCCIC Incident Reporting System provides a secure, web-enabled means of reporting cybersecurity incidents to the NJCCIC. The information you submit allows us to provide timely handling of your security incident, as well as the ability to conduct improved analysis. If you would like to report a cybersecurity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

Reporting Suspicious Activity

Suspicious Activity Reporting

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

Public Engagement



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

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

Information Sharing

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

Report Suspicious Activity

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

☎ **1-866-4-SAFE-NJ (866-472-3365)** ✉ tips@njohsp.gov 🌐 njohsp.gov/njsars

In The News

On September 30, 2021, a student reported to school authorities about seeing a picture of a bomb along with a threat toward a school in Mercer County. Police were notified immediately and as a precautionary measure, nearly 1,000 students were safely evacuated and sent home early. The high school was searched and secured, and three suspicious packages were found but later cleared. Although the threat was later deemed non-credible, the incident highlights how successful the suspicious activity reporting process works in the State and how it can assist in preventing violence.

NJ Office of Homeland Security and Preparedness

New Jersey Threat Assessment Glossary

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

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

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

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

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

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

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

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

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

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

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

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

Anarchist Extremists - Advocate violence in furtherance of movements such as anti-racism, anti-capitalism, anti-globalism, anti-fascism, and environmental extremism.

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

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

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

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

Black Racially Motivated Extremists (BRMEs) - Individuals or groups who believe in and/or advocate for the advancement of the black race over all others and use violence or criminal activity to further their ideology.

Botnet - A collection of connected devices, often within an IoT network, that become infected and controlled by malware to benefit cybercriminals.

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

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

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

Critical Infrastructure - System and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

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

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

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

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

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

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

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

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

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

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

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

Militia Extremists - View the federal government as a threat to the rights and freedoms of Americans. They judge armed resistance to be necessary to preserve these rights.

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

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

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

Racially Motivated Extremists (RMEs) - Individuals or groups who believe in and/or advocate for the advancement of one racial or ethnic group over all others and use violence or criminal activity to further their ideology.

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

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

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

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

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

Sovereign Citizen Extremists - Individuals or groups throughout the United States who view federal, state, and local governments as illegitimate, justifying their violence and other criminal activity.

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

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

Troll Farm - an organization set up in order to publish a large number of messages or posts on the internet, that often appear to be from people who do not really exist, and that are intended to cause trouble, influence political views, etc.

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

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

White Racially Motivated Extremists (WRMEs) - Individuals or groups who believe in and/or advocate for the advancement of the white race over all others and use violence or criminal activity to further their ideology.

NJ Office of Homeland Security and Preparedness

Recognize and Report

Signs of Terrorism-Related Suspicious Activity

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

NJ Office of Homeland Security and Preparedness

Report Suspicious Activity

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

Save Our Contact