2023

Threat Assessment

New Jersey Office of
Homeland Security and Preparedness

njohsp.gov | cyber.nj.gov

About Us

The New Jersey Office of Homeland Security and Preparedness (NJOHSP) is tasked with coordinating counterterrorism, 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, 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

In recent years, domestic and foreign threat actors' tactics have continued to evolve, substantially transforming the threat environment as witnessed by New Jerseyans and the nation. With threat prevention a key priority for the New Jersey Office of Homeland Security and Preparedness (NJOHSP), we continue to focus on countering terrorism and cyber threats while also addressing new concerns, such as disinformation and counterintelligence threats from nation-state actors.

NJOHSP forecasts that homegrown violent extremists and white racially motivated extremists will remain the highest terrorist threats to New Jersey in 2023. Extremists will use mainstream and alternative social media platforms to coordinate attacks and radicalize sympathizers, who in turn will coerce populations and create unrest among the general public.

Another area of concern is that state and non-state entities are seeking to sow discord in the United States by circulating disinformation and misinformation in order to alter public perception, influence global affairs, and spread falsehoods. Our Office, in tandem with our partners, will monitor and address these threats as they arise through our Disinformation Portal and other intelligence products.

For the cyber domain, the threat landscape is constantly changing, and our New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) warns that ransomware will continue to be a costly and debilitating cyber threat, along with persistent targeting of user account credentials, and concerns related to supply chain vulnerabilities that cyber threat actors can exploit.

NJOHSP will face these challenges head-on and with the same resolve demonstrated in the past. We can build resiliency, share information among our partners, educate the public, and identify and forewarn of potential threats to the best of our ability. This is achieved through the administration of security-enhancing grant programs and our collaboration with public- and private-sector partners. Our work with the Interfaith Advisory Council (IAC) and its Executive Committee represents a whole-of-community approach aimed at mitigating threats against the state's diverse religious communities while encouraging valuable relationships with law enforcement. On the cyber front, NJCCIC will remain the State's foremost leading expert on cybersecurity and engage with stakeholders to promote best practices and resiliency.

In closing, we are grateful to all our partners who contributed to NJOHSP's 2023 Threat Assessment. As always, we remain committed to ensuring the safety and security of our State, its residents, and its visitors. Recognizing the public as one of our first and best lines of defense in the fight against terrorism, I would ask you all to stay vigilant and remind everyone, 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 2023

Table of Contents

2023 Assessed Threat Level **3**

High Threats in 2023 ..... **4**

HVEs Promote Coordination, Training, and Attacks 5

HVEs: 2022 Regional Arrests 6

WRMEs Exploit Military Capabilities 7

Domestic Terrorism **8**

Domestic Terrorism Overview 9

2022 Domestic Extremism Attack Timeline 10

Domestic Terrorism Threat Summary 11

Foreign Terrorist Organizations **14**

Zawahiri's Death Has Little Impact on AQ Operations 15

ISIS Strives to Retain Position as Premier Global Terror Group 16

Social Media **18**

Social Media Amplifies Radicalization and Disinformation 19

Cybersecurity Threats **22**

Critical Infrastructure **26**

Extremists Leverage Vulnerabilities of Soft Targets 27

New Jersey's Jewish Population Faces Multifaceted Threat 28

Resources **30**

Interfaith Advisory Council 31

New Jersey Shield Program 32

New Jersey Cybersecurity and Communications Integration Cell 33

Vetting Disinformation 34

Reporting Suspicious Activity 35

Terrorism Definitions **36**

Information Cutoff: February 1, 2023

New Jersey's Assessed Threat Level in 2023

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
	Al-Qa'ida in the Arabian Peninsula (AQAP)
	Animal Rights Extremists
	Environmental Extremists
	HAMAS
	Hizballah
	ISIS

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

Changes from 2022

Abortion-Related Extremists: This threat category was added after examining the actions of individuals and groups who justify violence against people and establishments representing opposing views on abortion. This encompasses pro-life and pro-choice extremists.

High Threats in 2023

HVEs Promote Coordination, Training, and Attacks

Despite declining numbers, homegrown violent extremists (HVEs) remain a high threat due to their commitment to planning targeted violence against perceived opponents and organizing tactical training operations, while using social media to coordinate attacks and share personal grievances to justify violence. In the tristate area, authorities arrested five individuals that committed two attacks, one plot, and two instances of material support.

In November, authorities arrested Omar Alkattoul of Sayreville (Middlesex County) for using social media to share a manifesto containing a threat to attack a synagogue. According to the criminal complaint, Alkattoul researched mass shootings and methods for weapons acquisitions and stated his intent to conduct a "shooting attack." In his manifesto, Alkattoul claimed that Jewish people were responsible for Muslim hatred in the West. He viewed propaganda online and recorded himself pledging allegiance to ISIS and its recently deceased leader. Alkattoul also empathized with and drew motivation from white racially motivated extremist Dylann Roof, who targeted black Christians. In addition to his desire to target a synagogue, he also stated he would attack a gay club.

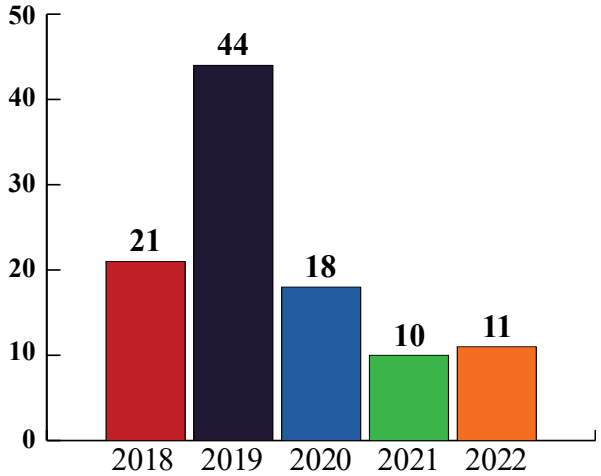
Understanding the HVE Threat

HVEs consistently show a propensity to conduct violence and provide material support for foreign terrorist organizations.

HVEs are individuals inspired—as opposed to directed—by foreign terrorist organizations and radicalized in the countries in which they are born, raised, or reside. These organizations continue to call for attacks in the West despite these groups' inability to execute large-scale attacks in recent years.

In August, authorities arrested Herman Wilson for attempting to provide material support to ISIS. Wilson, also known as Bilal Mu'Min Abdullah, attempted to set up an "Islamic State Center" in Albuquerque for individuals who wished to fight for ISIS. His goal was to teach ISIS ideology, provide training and martial arts skills, and for the center to serve as a safe haven for individuals preparing to travel and fight for ISIS. Wilson also ran an online platform that discussed ISIS ideology, reviewed attacks in the US and overseas, and promoted the training center. He later tried to shut down the platform to impede the federal investigation.

Identified HVEs by Year*



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

In February 2022, authorities arrested Maine resident Xavier Pelkey for possession of improvised explosive devices (IEDs). In November, federal authorities also charged him with providing material support to ISIS. Authorities found three homemade IEDs in Pelkey's bedroom, as well as a hand-painted ISIS flag. Pelkey, along with two unidentified juveniles, located in Illinois and Kentucky, planned to attack "an identified Shia Muslim mosque in the Chicago area" or a synagogue. The subjects had coordinated all attack details exclusively via social media over the course of three months. Pelkey planned to bring the IEDs, firearms, and ammunition to Chicago in March 2022, when he would meet the juveniles to conduct the attack. Pelkey allegedly wanted law enforcement to kill him so that he could die a martyr.

Omar Alkattoul Sayreville

In November, authorities arrested Omar Alkattoul of Sayreville (Middlesex County) after he shared a manifesto online containing threats to attack several locations and groups of people including a synagogue and gay club on behalf of ISIS. Additionally, Alkattoul supported Dylann Roof because he attacked Black Christians stating, "Muslims in the West should learn from him." Alkattoul found inspiration from ISIS as well as Anwar al-Aulaqi, a deceased cleric of al-Qa'ida in the Arabian Peninsula (AQAP).

Hadi Matar New York City

In August, Hadi Matar of Fairview (Bergen County) attacked author Salman Rushdie on stage at a lecture in Chautauqua, New York. Matar stabbed Rushdie multiple times in support of the Iranian Revolutionary Guard Corps. In 1989, Iranian Grand Ayatollah Ruhollah Khomeini issued a fatwa, or edict, calling for the author's death after Rushdie published a novel titled, "The Satanic Verses." Since publishing the book, Rushdie has been the center of protests across the Middle East. Rushdie spent many years in hiding due to the death threats.

Seema Rahman Edison | Abdullah At Taqi New York City

In December, federal authorities charged Seema Rahman of Edison (Middlesex County), Abdullah At Taqi of New York City and two others with conspiring to provide material support to ISIS. The four defendants raised funds for ISIS using a variety of methods, including cryptocurrency and crowdsourcing. According to the Department of Justice, the group tried to conceal its fundraising efforts by pretending the money was for "charitable sources."

Trevor Bickford New York City

On New Year's Eve, Trevor Bickford attacked and injured three NYPD officers with a machete. Prior to the attack, the FBI determined Bickford wanted to fight in Afghanistan and placed him on a federal watch list to prevent him from traveling overseas after his mother reported his radicalization. Bickford acquired a large sum of cash, packed a machete, and boarded a train to New York on December 29. Authorities stated that he intended to die and carry out an attack on "police officers or anybody in uniform."

White racially motivated extremists (WRMEs) will likely exploit military tactics, techniques, and procedures to gain combat experience, tactical training, and weapons proficiency. While WRMEs rely on recruitment of former and current military personnel, they also gain expertise through researching manifestos and online forums that justify their violent rhetoric and advocate attacking targets that oppose their views.

In August, authorities federally charged Killian Ryan for lying on his security clearance application. On that same day, he was discharged from the US Army for "serious misconduct." An investigation revealed Ryan had ties to social media accounts that were "associated with racially motivated extremism." He claimed he enlisted in the Army so he would be "more proficient in killing" black people and allegedly had numerous accounts where he communicated with other extremists.

In June, authorities arrested former Marine, Matthew Belanger, for using false statements to unlawfully obtain firearms. The FBI began investigating him in 2020 and found over 1,900 images related to "white power groups, Nazi literature, [and] brutality towards the Jewish community [and] women" on devices in his possession. He was allegedly the leader of a neo-Nazi group, which was planning to attack a New York synagogue, and members of the group claimed Belanger authored the group's manifesto. The document called the rape of women an "effective tool" to "increase the production of white children" to intimidate enemies. The manifesto also advocated for the harming and killing of "enemies of the white race," including attacks against the Jewish community and other ethnic groups. The military discharged Belanger from service in May 2021 due to "dissident/extremist activity."

In June, authorities arrested a former Ohio National Guard member, Thomas Develin, for making and selling untraceable homemade weapons. Develin made the weapons with a 3D printer and also possessed homemade conversion devices to convert rifles and pistols into fully automatic machine guns. Develin made numerous antisemitic and violent statements while employed to provide security services at local synagogues and Jewish schools. While working, he posted comments online saying, "I'm at a Jewish school and about to make it everyone's problem" and "the playground is about to turn into a self-defense situation." During a search of his residence, authorities discovered more than 25 firearms, two IED manuals, night vision goggles, ballistic plates, a ballistic helmet, first aid equipment, and a large amount of ammunition.

Case Study: Payton Gendron

WRMEs will seek inspiration from the success of past attackers and consult online manifestos for ideological and tactical guidance. On May 14, Payton Gendron livestreamed himself attacking a grocery store in Buffalo, where he killed 10 people and injured three others. Gendron claimed isolation during the COVID-19 pandemic exposed him to numerous racist ideologies online. Brenton Tarrant, the 2019 Christchurch, New Zealand mosque attacker who published a widely circulated manifesto online, inspired Gendron. Gendron wrote and shared his own manifesto, which largely borrowed from Tarrant's and expounded upon his own newly-formed extremist ideologies. His 180-page manifesto contained several racist and antisemitic memes and frequently referenced the Great Replacement Theory, which purports immigrants, through the actions of "Jewish elites," are replacing white people.

Payton Gendron

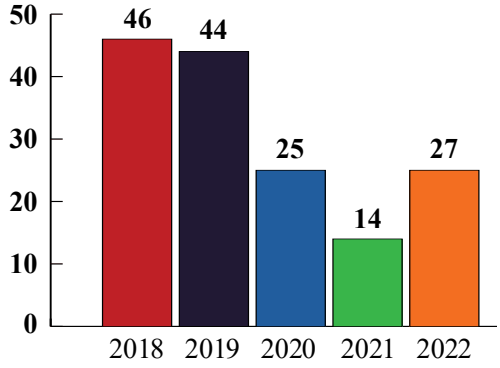
Domestic Terrorism

Domestic Terrorism Overview

An NJOHSP nationwide review of domestic extremist incidents in 2022, including attacks, threats, plots, and incidences of weapons stockpiling, highlights the enduring threat of lone offenders who identify with varying ideologies. In the past year, lone offenders with differing ideologies have used their personal grievances against religious groups, minorities, and law enforcement as justification for violence and spread of hateful rhetoric.

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

Incidents by Year*

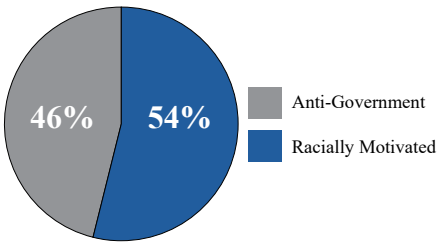


**This data only reflects publicly available information related to domestic terrorism incidents nationally and may be subject to change.*

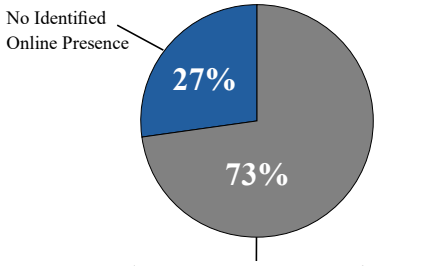
Domestic Extremist Attack and Plot Trends

In November, NJOHSP analyzed 13 domestic extremist attacks and plots linked to 15 individuals associated with racially motivated and anti-government extremist ideologies from January 1, 2021 to August 31, 2022. The assessment revealed notable statistics and trends among these subjects, including arrests and fatalities, methodology, social media engagement, and group affiliation. View the full report here: njohsp.gov/analysis/domestic-extremist-attack-and-plot-trends-2021-2022.

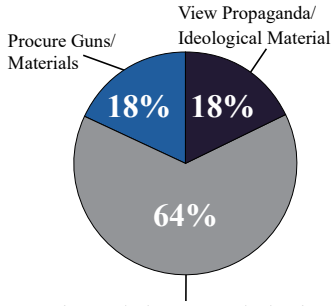
Ideological Affiliation



Social Media Presence



Use of Social Media



Key Findings (13 Incidents involving 15 Perpetrators)

**Chart depicts number of victims in attacks. 10 of the 13 killed were from one attack.*

Wrote Manifestos

Use of Body Armor

Utilized Improvised Explosive Devices

2022 Domestic Extremism Attack Timeline

April 8 HATE

Black Racially Motivated Extremist: Dion Marsh attacks four members of the Orthodox Jewish community in Lakewood and Jackson (Ocean County). Marsh assaults and carjacks a motorist and then strikes three pedestrians with two different cars. In one instance, Marsh exits the vehicle and stabs one of the victims. Marsh tells authorities upon his arrest that "it had to be done" and that Jewish people "are the real devils."

April 25

Sovereign Citizen Extremist: Law enforcement kills Micaiah Clinton at a truck stop near Aurora, Oregon, after he shoots at authorities and wounds an officer who attempts to arrest him on a federal warrant. Clinton carries an assault rifle loaded with armor piercing ammunition and wears a gas mask, body armor, and a badge that identifies him as a sovereign citizen.

May 14 HATE

White Racially Motivated Extremist: Payton Gendron shoots and kills 10 people and injures three at a grocery store in Buffalo. Gendron arrives at the store heavily armed, wearing tactical gear that includes a helmet with a camera attached while livestreaming the attack on Twitch, a video streaming platform. While in police custody, Gendron admits he planned to continue the attack beyond the grocery store if police had not intervened.

August 11

Anti-Government Extremist: Ricky Shiffer attempts to breach the entrance of the FBI's Cincinnati field office with a nail gun and assault rifle. After an alarm was set off and agents respond, he flees the scene in his vehicle. Authorities discover him on an interstate and fatally shoot him after a six-hour standoff.

Abortion-Related Extremists

Abortion-related extremists (AREs) will likely threaten groups that support or oppose government abortion legislation and may target reproductive healthcare facilities and religious institutions. Since the Supreme Court overturned Roe v. Wade on June 24, AREs have used incendiary devices and vandalism to target property.

In October, Joshua Brereton pleaded guilty to setting fire to a Planned Parenthood facility in Kalamazoo, Michigan, in July. In June, an unidentified attacker fire-bombed the Gresham Pregnancy Resource Center in Oregon.

Anarchist Extremists

Anarchist extremists will likely damage private and public property, exploit demonstrations to conduct riots, and attack law enforcement in opposition of governments, corporations, and various political movements. Supporters who engage in attacks rely on arson, vandalism, and black bloc tactics, which involve dressing in black clothing to conceal one's identity.

Throughout 2022, anarchist extremists sabotaged a personal vehicle belonging to a police officer who was involved in a fatal shooting and participated in direct action events to disrupt 2022 elections.

Anti-Government Extremists

Anti-government extremists, due to their distrust of government institutions and legislation will likely stockpile weapons, modify firearms illegally, and threaten government officials. Lone offenders who subscribe to various conspiracy theories have relied on firearms as their primary weapon to attack law enforcement officers who represent government authority.

In November, authorities arrested Aron McKillips of Sandusky, Ohio, a self-described Boogaloo member, for threatening federal law enforcement, as well as building homemade machine guns and stockpiling silencers and bomb-making materials. McKillips claimed he was also in possession of a grenade launcher and allegedly had plans to "blow up the IRS." In one recording, McKillips stated "Kill feds, kill police, kill government officials. Kill them. Murder them. Unalive them. Delete them. Get rid of them."

Black Racially Motivated Extremists

Black racially motivated extremists (BRMEs) are likely to target law enforcement and members of the Jewish community as well as participate in low-level criminal activity. In the past five years, BRMEs have primarily relied on edged weapons, small arms, and vehicles to carry out attacks.

In April, Dion Marsh targeted four members of the Orthodox Jewish community in four separate attacks in Lakewood and Jackson (Ocean County), injuring three and stabbing a fourth victim. After being charged criminally, prosecutors announced in June that Marsh would be indicted on terrorism charges.

Militia Extremists

Militia extremists will likely threaten and target government institutions and political figures whom they believe are acting unconstitutionally. Militia extremist propaganda heavily relies on conspiracy theories and other falsehoods.

In October, federal law enforcement officers arrested Darrian Nguyen, of Anoka, Minnesota, for illegally possessing a machine gun. Nguyen supported the Three Percenters militia movement and spoke of killing "liberals" and attacking Black Lives Matter supporters, according to the criminal complaint.

Sovereign Citizen Extremists

Sovereign citizen extremists, due to their belief in government and financial conspiracy theories, will likely harass public officials, reject judicial powers, and disregard law enforcement authority. Sovereign citizen extremists have conducted opportunistic attacks to evade arrest and also use fictitious legal documents to avoid prosecution.

In September, authorities arrested Darris Moody of North Carolina for placing $10,000 kidnapping bounties on numerous local officials. Open-source reporting revealed Moody mailed her victims a fictious judgement she acquired on a common law website that adheres to using unwritten laws. It was reported that almost 1,000 public servants from 41 states and the District of Columbia received similar letters.

NJ Office of Homeland Security and Preparedness

Foreign Terrorist Organizations

Zawahiri's Death Has Little Impact on AQ Operations

Amidst uncertainty surrounding its leadership succession, al-Qa'ida (AQ) operations will persist uninterrupted as the group remains focused on the growth of its affiliates in Africa, efforts to demonize the West to inspire attacks, and the production of extensive propaganda targeting perceived enemies. In July, the US killed former AQ leader, Ayman al-Zawahiri; however, AQ supporters online were not discouraged and claimed, "there are a thousand Aymans" ready to step forward.

AQ's influence in Africa has grown with its Somalia branch, al-Shabaab, gaining prominence within the region. Al-Shaabab is expanding into Kenya and is allegedly responsible for helping finance AQ operations worldwide through illicit trading and extortion. In October, the US Treasury added several al-Shabaab financial facilitators to the sanctions list[1] in order to disrupt the group's support network, claiming they "engaged in weapons procurement, financial facilitation, and recruitment activities for al-Shabaab." Jama'at Nasr al-Islam wal Muslimin (JNIM), another African AQ affiliate, has conducted various attacks in Mali and Burkina Faso and is seeking to establish and expand its own form of governance in the region.

In September, AQ released the fourth issue of its English-language version of *One Ummah*, alleging the "imminent collapse" of America. The magazine also claimed the Islamic world is under attack from the US, and that the response should be to "hunt down America and its allies." In August, AQ issued a response to the US bilateral meeting with leaders in Saudi Arabia which implied the US is "deepening the rift between Muslims" and seeking to harm Islam. Beginning in February 2022, AQ sympathizers started issuing a new magazine titled, *Mujahideen in the West*, which encouraged followers to act against enemies in the US and to focus on hard targets to better maximize damage.

For the anniversary of the 9/11 attacks, as-Sahab Media Foundation, the group's official media outlet, published various videos and products, including a booklet claiming that AQ's actions "ignit[ed] the flame of Crusader conflict" and continues to inflict long-term harm on the US. In August, the group also released the seventh issue of the Arabic version of *One Ummah*. The 70-page publication shared a supplemental of a former leader of its al-Qa'ida in the Islamic Maghreb affiliate, and highlighted the potential expansion of al-Shabaab in Somalia.

[1]US Treasury's Office of Foreign Asset Control coordinates several different sanctions programs and lists, including the Specially Designated Nationals and Blocked Persons lists. The US can use the sanctions to block assets and enforce trade restrictions.

Al-Qa'ida Under Ayman al-Zawahiri's Leadership

On July 31, Ayman al-Zawahiri was killed in a US drone strike in Kabul, Afghanistan. Before the strike, the US government had tracked his movements in and out of Afghanistan in the months prior. Neither AQ core nor its affiliates have confirmed his death.

Under Zawahiri's leadership, AQ claimed responsibility for one attack on US soil, which occurred on December 6, 2019, at the Pensacola Naval Air Station in Florida and resulted in three dead and eight individuals injured. During his tenure, Zawahiri largely focused on propaganda, often calling for violence against the West.

AQ has grown its network of affiliates during Zawahiri's leadership. These affiliates include al-Qa'ida in the Indian Subcontinent, which formed in 2014; JNIM, which had previously been four groups that merged under an AQ flag in 2017; and al-Shabaab, which officially pledged allegiance to AQ in 2012.

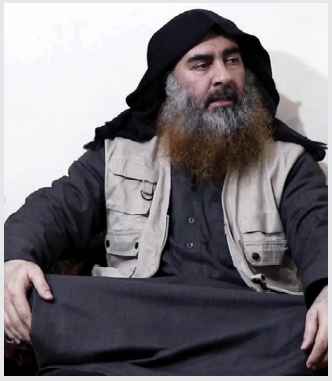
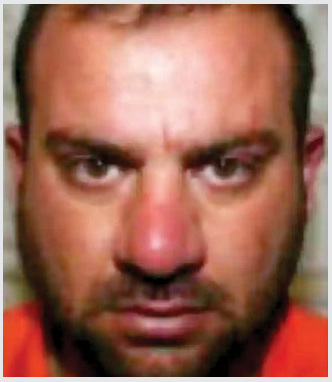
ISIS will likely leverage its affiliates to bolster its appeal to Western audiences and revitalize its membership to improve operational performance, all while attempting to inspire attacks from sympathizers globally. In November, ISIS spokesman Abu Umar al-Muhajir released an official statement announcing the death of the group's leader, Abu al-Hassan al-Hashimi al-Qurayshi. In the statement, al-Muhajir named Abu al-Husayn al-Husayni al-Qurayshi as the successor.

Over the last year, ISIS Khorasan (ISIS-K) has attempted to appeal to foreign supporters outside of its typical area of operations. In January 2022, a pro-ISIS-K group began producing an English-language magazine titled, *Voice of Khurusan*. Since its inaugural issue, the group has published 18 versions with the most recent in January becoming ISIS' primary English-language propaganda. The magazine covers a variety of topics ranging from regional issues to discussing cultural and political concerns in the United States. In its July issue, the magazine discussed gun violence in the US, referring to it as "divine retribution" and announcing that there will be a reestablishment of the ISIS caliphate.

In November, in its *al-Naba* newsletter, ISIS released an article titled, "Proceed on Your Path, Even if You are Alone." The article calls for "strong men" to join its ranks and encourages supporters to continue despite setbacks. The newsletter also states, "beware of instant gratification, for the road is long and lonely, and it is covered with blood and heavy trials." Additionally, in September, ISIS released a speech through its *al-Furqan Media Foundation*. In the speech, al-Muhajir claimed ISIS is committed to its fight and also congratulated ISIS West Africa and Central Africa on their operations and prison releases. Al-Muhajir called for all ISIS affiliates to look toward its African affiliates as an example. Lastly, he called for Muslims worldwide to join ISIS as the rest of the world has "insulted your religion for a long time."

In September, ISIS-K propagandist Abu Khurasan al-Mujahid released six audio messages titled, "Lone-wolf Attacks on the Dar al-Kufr [Land of Disbelief]" in which he outlined three specific reasons for ISIS supporters in the US and Europe to conduct attacks. Al-Mujahid stated that attacks in the West protect the "global Muslim Ummah," can spark civil war in the West, and dissuade Muslims from immigrating. He claimed, "whenever the Caliphate's followers kill a few Kafirs [disbelievers]…America divides into two camps: Racist-Nationalists and Democrats."

ISIS Leadership History

			
Abu Bakr al-Baghdadi June 2017-September 2019	Abu Ibrahim al-Hashemi al-Qurayshi October 2019-February 2022	Abu al-Hassan al-Hashimi al-Qurayshi March 2022-October 2022	Abu al-Husayn al-Husayni al-Qurayshi November 2022-Present

NJ Office of Homeland Security and Preparedness

Social Media

Domestic and foreign threat actors leverage mainstream and alternative social media platforms and encrypted messaging applications in an attempt to radicalize and motivate sympathizers as well as sow discord and panic among New Jersey residents.

Domestic Threat Actors

Domestic extremists will likely use mainstream and alternative social media platforms to encourage violent attacks, procure weapons, and view propaganda and ideological material. In April, a US-based research center published a study that found that extremist use of social media mirrors the general population, where they use a variety of social media platforms and focus mainly on mainstream applications.

On August 11, Ricky Shiffer attempted to breach the FBI Cincinnati field office. He used an alternative social media platform to share messages about lack of trust in government institutions. Following the FBI's search of former President Donald Trump's home on August 8, Shiffer posted, "Be ready to kill the enemy" and "get whatever you need to be ready for combat." He also suggested "killing" federal agents who tried to stop them.

Shiffer posted to an alternative social media platform prior to the attempted breach.

In June, federal authorities arrested Matthew Belanger for firearm-related charges. Belanger discussed neo-Nazi ideology on an encrypted messaging application and used social media to conspire with others, including members of a group called Rapekrieg. Belanger used a Facebook profile with the name "Adolf Hitler" to procure guns, including an assault rifle and pistol, and to plan hate crimes, including an attack on a New York synagogue. Disguised as a Jewish man, Belanger also managed a Twitter account to generate hate towards the Jewish community.

According to an NJOHSP review of terrorism cases in the tri-state area (New Jersey, New York, and Pennsylvania), social media played an integral role in 23 threat actors' motivations to carry out 21 attacks and plots from 2018-2022. Cases included racially motivated and homegrown violent extremists.

On May 14, Payton Gendron shot and killed 10 individuals, and injured three others inside a grocery store in Buffalo. Prior to the attack, Gendron used 4chan, an alternative anonymous online imageboard, to research and engage with white racially motivated extremist material, including manifestos and videos of previous attacks. In his manifesto, Gendron highlighted the role online racist and antisemitic content played in his radicalization, writing, "I simply became racist after I learned the truth."

As mainstream platforms continue to increase content moderation efforts and remove accounts that violate their guidelines, extremists are likely to seek alternative platforms such as Gab, Truth Social, and Parler.

Foreign Threat Actors

Foreign threat actors leverage social media to influence and control their population, improve their image, and advance strategic objectives on the global stage. The RAND corporation estimates that foreign influence campaigns will likely increase over the coming decade and pose a higher risk to smaller social media platforms than to mainstream sites.

Iran heavily regulates and bans many social media platforms, but has allowed the use of Instagram and other platforms to promote economic growth and cyber propaganda and to systematically monitor and exploit influencers' accounts, according to a US-based think tank. Iranian security and intelligence agencies have forced celebrities and others to post messages encouraging citizens to stop protesting. Since September 16, Iran has faced protests after the country's morality police killed Mahsa Amini while in custody for not wearing her hijab correctly and wearing "skinny" jeans. According to the Associated Press, as of December 21, Iranian security forces have killed at least 506 people and arrested over 18,000.

Following the invasion of Ukraine, the Russian government actively sought to control social media to repress speech and assembly. Roskomnadzor, the country's internet and media regulator, played a critical role in controlling the internet by managing a website blocklist with over 1.2 million URLs and ordering Facebook, Instagram, TikTok, and other platforms to censor content. The organization also actively surveilles individuals residing in the country.

In September, Meta, Facebook's parent company, disrupted the first known China-based political influence operation, which was targeting users in the US. Leading up to the midterm elections, Meta identified Facebook, Instagram, and Twitter accounts focusing on divisive topics, such as abortion and gun control. The operation targeted both political parties and shared politically-charged memes and interacted with posts from public figures since at least November 2021.

Disinformation

State and non-state threat actors will likely use social media to spread false narratives with the intent of misleading the public, shaping perspectives, and influencing global affairs. In October, a US-based organization found that Twitter and TikTok are the greatest social media amplifiers of misinformation due to their content sharing and predictive algorithms. In September, NewsGuard, an organization that tracks the problem online, reported that nearly 20 percent of the videos presented as search results on TikTok contained false or misleading information on topics such as school shootings and Russia's war in Ukraine.

In December, Stanford University released a report identifying suspected Russian actors leveraging alternative social media platforms to sow divisive political narratives in the US. Researchers identified a network of 35 inauthentic accounts on Gab, Gettr, Parler, and Truth Social that connected to previously identified foreign influence operations.

In October, a cybersecurity firm found that the People's Republic of China (PRC) was operating a disinformation influence campaign, known as DRAGONBRIDGE, with the goal of supporting the political interests of the PRC. Targeting the US, DRAGONBRIDGE attempted to sow division between the US and its allies, and within the US political system, claiming that APT41, a PRC-sponsored hacking group, is actually a

US government-backed threat actor. The campaign also attempted to discourage Americans from voting in the 2022 elections and alleged that the US was responsible for the Nord Stream gas pipeline explosions.

The same month, Russian-controlled social media accounts shared dozens of videos in as many as 18 different languages to spread conspiracy theories, including claims that Ukraine is responsible for civilian casualties and that Ukrainian residents welcomed Russian soldiers, according to a US-based intelligence firm. Examples of these propaganda videos were identified on Twitter, Gab, and Truth Social. Law enforcement also identified state-sponsored media on Telegram intended to remove any identifiable links between that content and Russia.

Disinformation Portal

In 2022, NJOHSP unveiled an updated disinformation portal focused on assisting the public in identifying and vetting any truth-obscuring, manufactured information. The disinformation portal examines tactics, techniques, and procedures that nation-state and non-state entities engage in, sometimes referred to as psychological operations. Disinformation has the potential to incite panic, create distrust between the government and people, increase polarization, influence government actions or law enforcement responses, exhaust resources, and cause undue harm.

What is Disinformation?

Disinformation: manufactured information that is deliberately created or disseminated with the intent to cause harm, obscure the truth, or influence public opinion.

How is Disinformation Identified?

NJOHSP strongly urges the public to reference legitimate and credible organizations for accurate information and to fact check claims from competing sources. Several indicators to identify misleading postings include accounts that:

- Lack personal information and/or a username that contains numbers, hashtags, or emojis
- Include a high level of postings (more than 100 per day)
- Post messages throughout the day and night
- Use more than one language
- Follow suspicious accounts
- Use a default profile picture
- Contain misspellings, recently created accounts, and/or unfamiliar website links

It is highly recommended that the public reports any posts containing threats, calls to action, or potential violence to local law enforcement as soon as possible. Suspicious activity with a possible nexus to terrorism should be reported immediately to NJOHSP's Counterterrorism Watch at 1-866-4-SAFE-NJ or tips@njohsp.gov.

Cybersecurity Threats

The New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) assesses with moderate confidence that the overall cyber threat to New Jersey is high. Throughout 2022, cyber attacks affected organizations, governments, businesses, and private residents in New Jersey. Ransomware, credential theft, and social engineering remained top cyber threats, with many attacks highlighting supply chain issues and interdependencies that increase vulnerability to these attacks.

RANSOMWARE

Ransomware impacted all critical infrastructure sectors, including government, healthcare, finance, and education in 2022. Ransomware attacks can affect citizen welfare, organizational operations, and the overall health of businesses or government departments. Several incidents impacted New Jersey businesses and organizations, including a ransomware attack targeting Somerset County in May. The incident caused a shutdown of all computers and required employees to create temporary personal email accounts to ensure the public could still contact health, emergency, and sheriff's departments. During the incident, county databases were unable to provide information on land or probate records, and title searches were only available for paper records entered before 1977. In one of several incidents impacting school districts, a ransomware attack affecting the Tenafly School District in June caused the cancellation of final exams as students and teachers were unable to access necessary files. Ransomware attackers also victimized many small and medium-sized businesses in New Jersey, further challenging their ability to operate amid shutdowns and staffing shortages.

In early 2022, a significant ransomware attack on Bernalillo County in New Mexico caused many government buildings, educational institutes, and correctional facilities to be shut down. The cyber attack impacted a jail's electronic cell door locking systems and security cameras, forcing the detention center to file an emergency notice in federal court.

Another crippling ransomware attack occurred against the government of Costa Rica, forcing a national emergency declaration. It was the first time a country made such a declaration in response to a cyber attack. The attack began in early April and shut down the Ministry of Finance and many government services, along with private-sector entities engaged in imports and exports. The ransomware threat group, Conti, took responsibility for the attack, demanding the government pay a ransom of $20 million. On March 31, a separate attack linked to HIVE ransomware affected the country's healthcare system, taking it offline and impacting the Costa Rican Social Security Fund.

The energy sector also experienced several ransomware attacks. An attack on German oil company, Oiltanking GmbH, impacted 233 gas stations across Germany, forcing the company to revert to manual processes and reroute supplies to different depots. In addition, a HIVE ransomware attack impacted Perusahaan Gas Negara, Indonesia's state-backed oil and gas company that provides gas for 84 million customers. The threat actor behind the attack leaked data stolen from the company's network.

The cost of a ransomware incident far exceeds any ransom demanded when factoring in remediation expenses, fraud prevention or identity theft protection, and other associated recovery costs, in addition to reputational and public confidence losses. Ransomware is a significant cyber threat that demands organizations increase their cybersecurity posture to become more resilient to its potential impacts.

GEOPOLITICAL CYBER THREATS

The inapplicability of national borders in cyberspace, the commoditization of offensive cyber weapons, a hyperconnected world with an increasingly vulnerable attack surface, and heightened geopolitical unrest are all elements that raise the likelihood of nation-state or state-sponsored cyber threat activity, which could adversely impact New Jersey.

Russia's invasion of Ukraine increased concerns of retaliatory cyber attacks that may target key energy supplies in response to sanctions against Russia and monetary and weapons support provided to Ukraine. While state-sponsored groups have demonstrated the capability and intent to launch cyber attacks that cause physical damage to energy infrastructure, New Jersey's energy sector is more likely to face reconnaissance and intelligence collection activities aimed at exfiltrating data and establishing persistence on high-value networks for potential use in future sabotage operations. New Jersey's high-risk level is largely due to its significance as a major distribution center for petroleum products throughout the Northeast. New Jersey is home to three operating oil refineries and five key interstate natural gas carrier pipelines.

Throughout 2022, nation-state actors targeted key organizations within the government and defense industrial base sectors. Generally, nation-state actors carry out cyber attacks to advance their foreign policy interests and increase their influence on the world stage while decreasing that of their adversaries. Motivations include espionage and exfiltration of intellectual property, disruption and destruction of information and systems, sowing social discord, and financial gain.

While nation-state actors are considered advanced adversaries, they typically gain access to target networks by employing the same techniques used by individual cyber criminals and cyber criminal syndicates, hacktivists, terrorist groups, and other threat actors. These actors take advantage of simple passwords, unpatched systems, and unsuspecting computer users to gain initial access to systems before burrowing more deeply to gain persistence and carry out their objectives. Such attacks ultimately lead to the loss of critical information and information systems that could threaten public health and safety, undermine public confidence, have a negative effect on the economy, and diminish the security postures of the State of New Jersey and the United States.

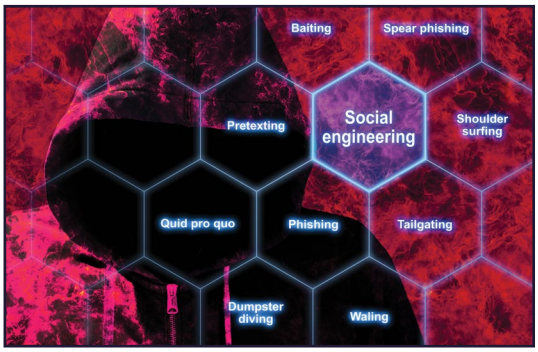
CREDENTIAL COMPROMISE

Account credentials – username and password combinations – provide threat actors with network access or the ability to launch subsequent cyber attacks, including ransomware. In March, cyber threat actors impersonated East Windsor, (Mercer County) township staff in phishing emails sent to other township staff in a successful effort to steal user account credentials and compromise accounts. These compromised accounts were then used to send phishing emails to the account's contacts, including private residents.

The average person has over 100 online accounts and often reuses passwords. While the risk of password reuse may seem miniscule to some, it can be the catalyst to a significant cyber attack. In 2021, a cyber threat actor gained access to the corporate network of Colonial Pipeline using an exposed password for a VPN account. This led to a ransomware attack that forced the company to halt operations for several days, causing a temporary gas shortage along the East Coast. If the VPN account was protected with multifactor authentication (MFA), Colonial Pipeline would have been notably more resilient to unauthorized access attempts.

Password managers can assist with creating and storing strong, unique passwords for each account, and MFA greatly increases account security. Users are highly advised to enable MFA, as it helps prevent unauthorized users from accessing accounts with only the password. If an unauthorized user does not have the account holder's second factor, they will be unable to access the account. Choosing an authentication application or hardware token when establishing MFA is recommended, where available.

SOCIAL ENGINEERING



Threat actors use various tactics and techniques in social engineering schemes to steal user credentials and other sensitive information, deliver malware, or dupe victims into providing funds to the perpetrator. Most cyber incidents have a human nexus that requires an action for the attack to be successful. The types of social engineering scams often observed include email phishing, business email compromise, vishing (voice phishing), and SMiShing (SMS text phishing).

Reporting received by the NJCCIC indicates social engineering campaigns carried out on social media platforms increased in 2022, leaving legitimate account holders without access and their contacts as targets of subsequent social engineering attacks. Private residents and businesses have incurred substantial losses to various social engineering schemes, including fraudulent invoice payment requests, gift card scams, payroll diversions, and account takeovers.

DEPENDENCIES

This past year also highlighted how interdependencies in technology can have lasting implications for cybersecurity. Third-party products and services used by companies can create a dependency reliant on the accessibility of those commodities to complete tasks and operate fully. If a cyber attack impacts one of these third parties, an inaccessible product or service could provide threat actors with an opportunity to target their clients. Organizations may need to better understand their overall cyber risk to incorporate variables for these dependencies.

The top three serious interdependencies exploited in 2022 were ProxyLogon, Log4Shell, and ZeroLogon. ProxyLogon – could allow threat actors to bypass authentication, read emails, and deploy malware in enterprise networks. Log4Shell, a critical flaw in open-source logging framework, Log4j, which developers use to track activity within an application, has left countless products and services vulnerable to threat actors through ransomware, cryptocurrency mining, and other malicious cyber activity. Lastly, ZeroLogon is an elevation of privilege flaw that malicious actors can leverage to compromise other devices on a network, including extracting all domain passwords.

Critical Infrastructure

Extremists Leverage Vulnerabilities of Soft Targets

Domestic extremists prioritize attacking soft targets as they are easily accessible and have limited security or protective measures. New Jersey's soft targets include community festivals, shopping centers, schools, transportation systems, and houses of worship. From 2018 to 2022, domestic and homegrown violent extremists carried out 16 attacks on soft targets killing 60 and injuring 66.

Extremists that attack soft targets tend to use easily acquired weapons like firearms, edged weapons, and vehicles. These methods provide ways for extremists to exploit vulnerabilities and attack these locations with little or no planning or expertise.

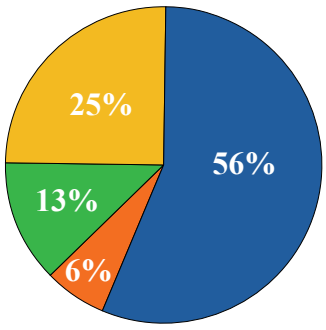
In May, Payton Gendron, attacked a grocery store in a predominately black neighborhood of Buffalo, killing 10 and injuring three. The day before the attack, Gendron conducted surveillance on the exterior of the building and interacted with customers asking for change, resulting in the store's manager telling him to leave. Prior to the attack in March, Gendron visited the store three times to test and record his observations of patrons, noting the store's entry points and limited security presence. On Discord, Gendron discussed attacking other soft targets, including black churches and schools. According to federal authorities, he chose the grocery store because of the "high percentage and high density of black people."

In July 2019, Santino Legan attacked the Gilroy Garlic Festival in California, killing three and wounding 17. Legan died from a self-inflicted gunshot wound. Legan leveraged the event's limited security measures and cut through a fence to avoid entering the security checkpoint, which used a metal detector as part of the entry requirements. Federal authorities found Legan created a list of soft and hardened targets, including religious institutions, political groups, federal buildings, and courthouses.

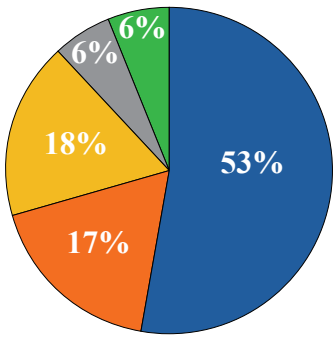
In October 2018, Robert Bowers opened fire at a synagogue in Pittsburgh, killing 11 and injuring six individuals. Three separate congregations used the Tree of Life Synagogue, including Dor Hadash, which openly supported the Hebrew Immigrant Aid Society (HIAS). Bowers expressed hatred for HIAS on social media sites, making antisemitic and anti-immigrant statements.

Attacks on Soft Targets, 2018-2022

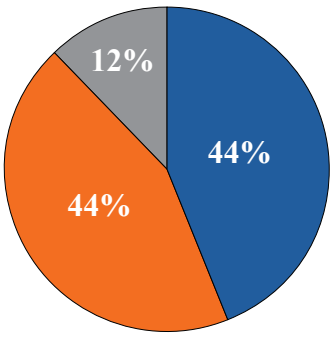
Ideology



Attack Method

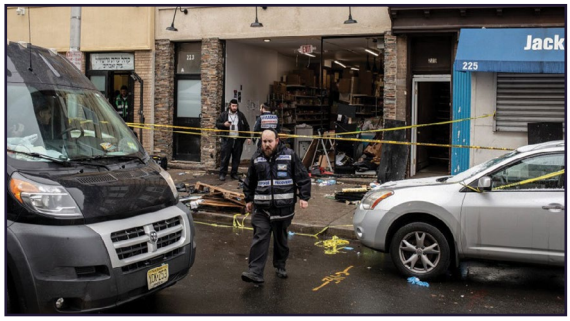


Sector Attacked



Racially motivated and homegrown violent extremists are motivated to target and carry out attacks on New Jersey's Jewish community due to shared antisemitic beliefs among corresponding ideologies. Notable US attacks on the Jewish community include the October 2018 Tree of Life Synagogue shooting in Pittsburgh, the April 2019 attack on a Chabad house in Poway, California, the December 2019 attacks in Jersey City (Hudson County) and an unrelated attack on a private Hanukkah celebration in New York City. According to a 2018-2022 NJOHSP review, extremists targeted the Jewish community nationally in seven attacks and in at least 11 publicly identified plots.

In November, federal and local authorities arrested two suspected white racially motivated extremists (WRMEs) in connection with online threats to attack a New York City synagogue. The suspects, Christopher Brown and Matthew Maher, "possessed a firearm, a high capacity magazine, ammunition, an 8" long military-style knife, a swastika arm patch, a ski mask and a bullet proof vest, among other things," according to the Manhattan district attorney. Following their arrests, Brown told authorities that he owned Nazi paraphernalia and operated a WRME Twitter group of which Maher was a member.



Aftermath of the December 2019 BRME attack on a kosher market in Jersey City (Hudson County).

In November, the FBI arrested Omar Alkattoul of Sayreville (Middlesex County) after he shared a manifesto in which he threatened to attack a synagogue and Jewish people. Alkattoul, a homegrown violent extremist, derived inspiration from ISIS and al-Qa'ida and planned to target a synagogue claiming that "Jews promote the biggest hatred against [Muslims]." According to authorities, Alkattoul wanted to target either a synagogue or gay club.

In April, Dion Marsh, a suspected black racially motivated extremist, conducted several violent attacks on members of the Orthodox Jewish community in and around Lakewood (Ocean County). The series of attacks occurred over the course of approximately seven hours and in residential areas where Marsh allegedly struck three men with a stolen vehicle, each in separate incidents, and stabbed another in the chest. According to the criminal complaint, when Marsh was asked why he conducted the attack, he stated, "it had to be done," and that "these [Jews] are the real devils."

Antisemitism

The member states of the International Holocaust Remembrance Alliance adopted a working definition at its 2016 plenary in Romania. This plenary agreed that "Antisemitism is a certain perception of Jews, which may be expressed as hatred toward Jews. Rhetorical and physical manifestations of antisemitism are directed toward Jewish or non-Jewish individuals and/or their property, toward Jewish community institutions and religious facilities." The most extreme example of antisemitism occurred during the Holocaust, the state-sponsored persecution and murder of European Jews by Nazi Germany and its collaborators between 1933 and 1945.

NJ Office of Homeland Security and Preparedness

Resources

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 New Jersey 21 counties, 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 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, law enforcement officials, as well as private- and public- sector managers of security, emergency management, and business continuity.

To become a member an individual should be a:

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

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

- 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 US 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.

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 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.

dis·in·for·ma·tion

manufactured information that is deliberately created or disseminated with the intent to cause harm, obscure the truth, or influence public opinion

Various actors, including state and non-state entities, attempt to spread disinformation in order to sow discord within New Jersey and elsewhere. Disinformation has the potential to exhaust resources, incite panic, create distrust between the government and people, increase polarization in groups, influence governmental actions or law enforcement responses, or cause undue harm, among other concerns.

Consider the Source

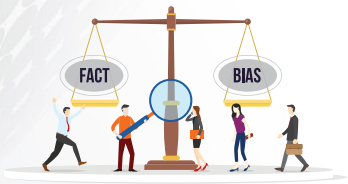
Who created the account or article or captured the original piece of content?

Check the Author's Motivations

Why was the account established, website created, or piece of content captured?

Check the Date

When was it created? Content, including pictures and videos, is often recycled and may not relate directly to the article.



Check Your Biases

What are your preconceived notions of the topic? Consider if your own beliefs may affect your view of the information.

Read Beyond

What is the whole story? Headlines can be misleading.

Supporting Sources

Where is the information from? Are you looking at the original account, article, or piece of content?

For more information on disinformation and other related topics, visit njohsp.gov/disinformation.

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 terrorism-related suspicious 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 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.

Terrorism-related 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 terrorism-related suspicious activity information 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

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.

Terrorism Definitions

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.

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.

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 US 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.

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.

Disinformation - Manufactured information that is deliberately created or disseminated with the intent to cause harm, obscure the truth, or influence public opinion.

Domestic Terrorism - Violence committed by individuals or groups primarily associated with US-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 end the Israeli occupation of Palestinian territory and establish a Palestinian state.

Hizballah - An Islamist militant group based in Lebanon and allied with Iran.

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.

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.

Pro-Choice Extremists - Individuals or groups who believe violence is justified to protect those who provide or receive reproductive health care services.

Pro-Life Extremists - Individuals or groups who believe abortion is unethical and that violence is justified against people and establishments providing abortion services.

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.

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

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.

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