2022

Threat Assessment

New Jersey Office of
Homeland Security and Preparedness

UNCLASSIFIED

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.

At the beginning of 2020, we reported homegrown violent extremism and domestic extremists as New Jersey's greatest threats. Prior to the 2020 Presidential election, NJOHSP forecasted a series of potential scenarios, prompting the release of a 2020-2021 Supplemental Threat Assessment. We expected online rhetoric and disinformation to fuel the convergence of the 2020 election, COVID-19 government response, and nationwide civil unrest. Subsequently in 2021, driven by anti-government sentiment, we witnessed the attack on the U.S. Capitol.

As we look toward the end of the pandemic, our analysts find that homegrown violent extremists and white racially motivated extremists remain high-level threats and that foreign terrorist organizations will seek opportunities to inspire extremists to conduct attacks in the Homeland or abroad. Additionally, numerous cybersecurity threats, such as ransomware and social engineering campaigns, will continue to impact residents and the public and private sectors.

We thank all our partners who contributed to NJOHSP's 2022 Terrorism Threat Assessment. In the next year and beyond, we reaffirm our commitment to securing New Jersey and doing everything possible to keep residents and visitors safe. It is important to note that the public is often our first line of defense in the fight against terrorism. I ask everyone to "See Something, Say Something" by reporting terrorism-related suspicious activity to our Counterterrorism Watch Desk at 1-866-4-SAFE-NJ and tips@njohsp.gov.

Sincerely,

Laurie R. Doran
Director, NJOHSP
February 2022

Table of Contents

Information Cutoff: February 1, 2022

New Jersey's Assessed Threat Level in 2022

High	Homegrown Violent Extremists
	White Racially Motivated Extremists
Moderate	Anarchist Extremists
	Anti-Abortion 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
	Islamic State of Iraq and Syria (ISIS)

NJ Office of Homeland Security and Preparedness

High Threats in 2022

HVE Threat High Despite Decreased Activity

Homegrown violent extremists (HVEs) remain a high threat to New Jersey in 2022, as they are driven to conduct attacks domestically, provide financial and messaging support, or attempt to travel overseas to fight on behalf of foreign terrorist organizations. In 2021, authorities arrested 10 HVEs, including a New York couple who attempted to board a cargo ship in Newark (Essex County) to travel to Yemen with prospects of joining ISIS.

In January 2021, authorities arrested Cole Bridges after he attempted to provide tactical guidance to an undercover FBI employee he believed was a member of ISIS. Bridges was an active-duty soldier who joined the Army in 2019 and began consuming online propaganda. He then started providing U.S. military manuals and guidance for ISIS fighters to attack soldiers deployed overseas. Bridges suggested attacking targets in the Homeland, such as New York City and the 9/11 Memorial.

Federal authorities arrested Benjamin Carpenter, of Knoxville, Tennessee, on March 3 for providing material support to ISIS. Carpenter is allegedly the leader of the pro-ISIS group, Ahlut-Tawhid Productions. The group dedicated itself to translating and producing pro-ISIS and official ISIS media in English to encourage English-speaking supporters. Carpenter attempted to provide the English-language productions to an undercover FBI employee, thinking ISIS would use it.

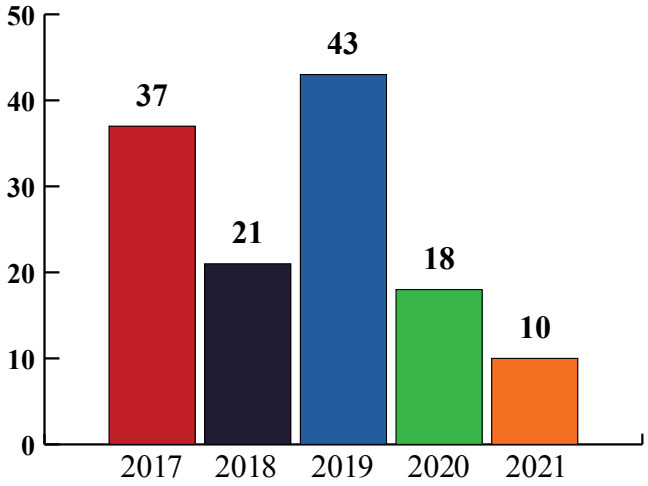
In March, authorities arrested James Bradley and his wife, Arwa Muthana, in Newark (Essex County) after they attempted to board a cargo ship traveling to Yemen to fight for ISIS. The couple also plotted against military targets in the event their travel was unsuccessful. Muthana is the sister of Hoda Muthana, an ISIS supporter from Alabama who traveled to join ISIS in November 2014. Additionally, in February 2021, authorities arrested Mohamed Suliman after he was expelled from Turkey and returned to the United States for attempting to cross the border into Syria. Suliman initiated his travel in June 2014 with the intent to enter Syria and join ISIS, but Turkish forces apprehended him before he reached Syria.

Understanding the HVE Threat

HVE support for foreign terrorist organizations is constant despite a decrease in arrests since 2020.

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 the groups' inability to execute large-scale attacks in recent years.

Identified HVEs by Year*



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

HVEs: 2020-2021 Regional Arrests

2020: Dzenan Camovic New York, New York

In June 2020, authorities arrested Dzenan Camovic for attacking law enforcement officers who were conducting anti-looting patrols in New York City. Camovic slashed an officer with a knife, stole his firearm, and fired multiple shots at responding officers. An investigation into Camovic revealed he supported violent Islamic extremism and possessed ISIS propaganda.

2021: Khaled Miah Pittsburgh, Pennsylvania

In January 2021, authorities arrested Khaled Miah for threatening and retaliating against federal law enforcement officers and obstructing a federal investigation. The FBI monitored Miah for over a year, during which Miah posted threats online against the FBI agents investigating him. He also repeatedly surveilled one of their homes. The investigation revealed Miah supported violent Islamic ideology, revered the Boston Marathon bombers, and possessed ISIS propaganda. A federal court found Miah guilty in December.

2021: James Bradley and Arwa Muthana Newark, New Jersey

In March, authorities arrested James Bradley and his wife, Arwa Muthana, for attempting to provide material support to ISIS. The couple discussed conducting terrorist attacks against the U.S. Military Academy at West Point and made plans to travel overseas to join ISIS. Authorities arrested Bradley and Muthana in Newark (Essex County) after Bradley paid an undercover law enforcement officer to gain passage on a cargo ship to take them to Yemen.

WRMEs Committed to Conducting Lone Offender Attacks

White racially motivated extremists (WRMEs) will likely produce personal manifestos, collect extremist literature and stockpile weapons while aspiring to conduct lone offender attacks. An NJOHSP review revealed that U.S.-based WRMEs conducted at least 28 attacks over the last five years, resulting in 52 deaths and 79 injuries.

In May, federal and state authorities arrested Coleman Blevins for plotting to conduct an attack at a Texas retail store. A local law enforcement officer discovered Blevins' plans after he posted his intentions on a social media platform. Law enforcement discovered WRME paraphernalia, firearms, ammunition, explosive chemicals, and handwritten documents. Following his arrest, several users on alternative online platforms began posting in support of Blevins and incorporating his picture into their propaganda.

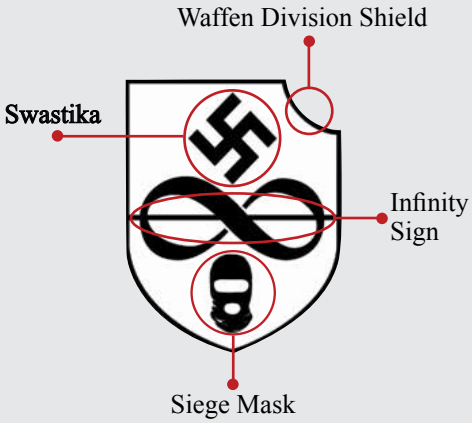
Items found in Blevins' apartment after his arrest

In June, Nathan Allen fatally shot a retired state trooper and a U.S. military veteran in Massachusetts, both of whom were black. Allen used multiple weapons and carried extremist literature that included numerous journal entries containing racist and hateful language. Allen's writings referenced the superiority of the white race and how whites are "apex predators" along with drawings of swastikas.

In July, law enforcement officers arrested Wesley Martines after discovering multiple weapons, body armor, ammunition, and an inactive improvised explosive device in his vehicle. Suspicious activity reporting led to Martines' arrest. Authorities recovered a journal that included racist and anti-Semitic writings stating how he wanted to wipe out specific minority and religious populations. Martines planned to "go to a sporting goods store, dress up as an employee, and tie everybody up." There were also bullets personally inscribed with phrases such as "Cop Killer," "First of Many," "A Good Start," and "To a widow from the Grim Reaper."

WRME Symbology

WRMEs often appropriate, alter, and adapt images and symbols from a wide variety of historical events, broader movements, religions, and popular culture. Co-opting imagery in this manner helps WRMEs convey their ideologies, recruit new members, intimidate opposing entities, and distinguish their group from others within the overall movement.



WRME symbol superimposed with various images

WRME organization patch found in Blevins' apartment

NJ Office of Homeland Security and Preparedness

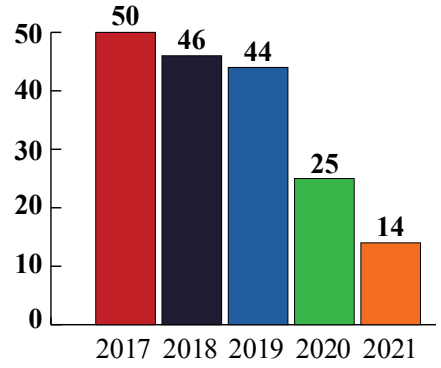
Domestic Terrorism

Domestic Terrorism Overview

Domestic extremists will likely return to pre-pandemic operating norms, shifting their focus toward local expansion, participating in demonstrations, and engaging in low-level criminal activity. Over the last two years, domestic extremists leveraged multiple national events to mobilize and justify violence throughout the United States.

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

Incidents by Year*



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

2021 Domestic Extremism Attack Timeline

January 6

Multiple domestic extremists: The total number of federal cases against individuals involved in the Capitol Hill insurrection stands at over 700. Nationally, individuals came from 46 states and the District of Columbia. Charges have been filed against 26 individuals from New Jersey, including 22 males and four females. As of February 1, five of the individuals plead guilty. Most individuals were unaffiliated with a group or ideology, and three were confirmed former military members.

April 17

Anti-government extremists: Four individuals assault a police officer during a protest in Washington, D.C. Following their arrest, police find Roman candles, bottle rockets, and other fireworks, as well as an ax.

June 21

Sovereign citizen extremist: Ronald Troyke ambushes and fatally shoots a police officer in Arvada, Colorado. Investigators discovered that the subject viewed anti-police videos online and wrote a note titled, "Sociopath Sovereign Citizens."

June 23

Black racially motivated extremist: Othal Wallace shoots and kills a police officer in Daytona Beach, Florida. Police discover he is affiliated with a black racially motivated extremist organization and participated in paramilitary training with the group.

June 26

White racially motivated extremist: After crashing a stolen box truck into a building in Winthrop, Massachusetts, Nathan Allen shoots and kills a retired Massachusetts state trooper and an Air Force staff sergeant. Following his arrest, police locate Allen's notebook that contains racist and anti-Semitic writings.

July 3

Sovereign citizen extremist: An armed group of sovereign citizens initiate a standoff with police on a highway in Wakefield, Massachusetts.

October 31

White racially motivated extremist: Franklin Sechriest sets fire to the Congregation Beth Israel synagogue in Austin, Texas. Following his arrest, police locate Molotov cocktail ingredients, Nazi propaganda, and a calendar containing anti-Black writing.

Anarchist extremists

Anarchist extremists will likely remain committed to abolishing government authority, disrupting commerce, and stifling economic growth. Supporters rely on vandalism and arson against public and private property to achieve these goals while also conducting attacks at gatherings to overwhelm law enforcement who attempt to curb their violence.

On June 1, Malik Fard Muhammad was federally charged with possessing an unregistered destructive device, engaging in civil disorder, and using explosives during violent protests in Portland, Oregon, in 2020. In September and October 2020, Muhammad allegedly provided baseball bats to violent protesters and threw multiple incendiary devices at police officers. An investigation into his activities revealed he traveled to Louisville, Kentucky, in August 2020 to conduct firearm and tactical training.

Anti-government extremists

Anti-government extremists' acceptance of conspiracy theories and distrust of elected officials and authority figures has likely motivated supporters to attack law enforcement, government institutions, and private-sector infrastructure that contributes to public safety.

In April, federal officers arrested Seth Pendley after he attempted to obtain an improvised explosive device from an undercover agent to attack an online retail data center in Ashburn, Virginia. Pendley used an encrypted messaging application to communicate with a confidential source. Following his arrest, Pendley stated that he believed the attack would "kill off about 70% of the internet" and disrupt service to the FBI, CIA, and other federal agencies. Additionally, he anticipated his attack would provoke members of the public to revolt against the president and members of Congress.

Black racially motivated extremists (BRMEs)

Black racially motivated extremists (BRMEs) will likely engage in low-level criminal activities, demonize law enforcement, and spread anti-Semitic conspiracies, while lone offenders may conduct isolated attacks. Violent lone offenders with various motivations have targeted law enforcement in opportunistic or ambush incidents, leading to several fatal attacks.

On June 23, Florida resident Othal Wallace fatally shot a Daytona Beach Police Officer while he investigated a suspicious vehicle. Authorities arrested Wallace, who subscribed to several BRME beliefs and previously attended a BRME-affiliated military-style training in Georgia.

Militia extremists

Militia extremists will likely plot independent attacks against government institutions, facilitate recruitment efforts, and encourage communication among followers and state chapters to exchange ideologies and spread disinformation. Over the last two years, supporters have exploited COVID-19 protocols to justify their violent ideologies and ongoing conspiracies that government officials are attempting to suspend civil liberties, necessitating a second civil war.

In July 2021, authorities charged two California residents, Ian Rogers and Jarrod Copeland, for plotting to destroy the John L. Burton Democratic Headquarters in Sacramento. Rogers and Copeland used multiple messaging applications to discuss attacking their target with incendiary devices, hoping their assault would motivate supporters to overthrow the government. During Rogers' arrest, federal law enforcement officers discovered approximately 50 firearms, thousands of rounds of ammunition, and five pipe bombs.

Sovereign citizen extremists

Sovereign citizen extremists' adherence to fictional statutes compel followers to challenge and reject certain laws and firearm regulations. While supporters have used violence to challenge authority figures, other members have conducted deadly attacks targeting law enforcement officers.

On December 4, police officers in Lumberton, Texas, arrested Jimmy Minter for evading arrest during a traffic stop, carrying an unlawful weapon, and making terroristic threats against a law enforcement officer. Minter sped away and resisted arrest after being pulled over for displaying a homemade license plate that read, "private citizen." During the incident, Minter threatened to kill the officer and refused to roll down his window, exit the vehicle, and provide his name and date of birth.

White racially motivated extremists (WRMEs)

WRMEs will likely continue to organize and operate as small cells or groups that fall under separate national banners. They will likely use social media as an avenue to spread their ideology, recruit new members, and communicate. Unaffiliated lone offenders may engage in isolated attacks against a specific facility or government target that they have a personal grievance towards.

In March, federal authorities arrested Paul Miller in Florida for felony possession of a weapon. The Anti-Defamation League reported Miller to authorities after he posted images online of various weapons and messages containing extremist rhetoric.

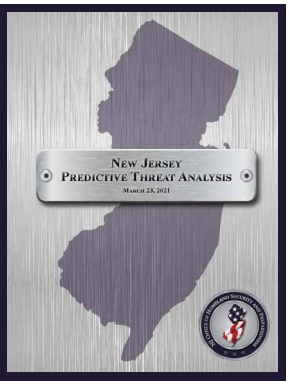
Blended Extremism

Over the last decade, certain extremists have leveraged the belief systems of multiple domestic extremists and foreign terrorist organizations, tailoring these systems to develop and ultimately form unique, radical worldviews that advance the individuals' violent goals. These extremists use this ideological convergence to justify violence against shared targets or for guidance while using common tactics, such as attack methods, recruitment strategies, and propaganda distribution. This phenomenon, coupled with the availability of various social media platforms, creates a unique security challenge for law enforcement.

In June 2020, federal authorities charged Ethan Melzer with planning an attack on his U.S. Army unit and sharing sensitive details with a neo-Nazi and WRME group. Melzer associated with the group that combines views of Nazis and Islamic extremists. He consumed propaganda from various WRME groups and ISIS.

On March 23, NJOHSP released a Predictive Threat Analysis product which assessed the intentions and likely direction of domestic extremists and homegrown violent extremists within New Jersey through 2024. The report takes into consideration the post pandemic operating environment. To view the report, please visit: www.njohsp.gov/analysis/new-jersey-predictive-threat-analysis.

NJOHSP maintains "terrorism snapshots" for all domestic extremist groups and the threats these organizations present to the State of New Jersey. For more information, please visit: www.njohsp.gov/terrorism-snapshots.



Domestic extremists will likely exploit encrypted messaging platforms and alternative social media applications to amplify extremist rhetoric, communicate and coordinate among like-minded individuals, and maintain followers across platforms. Alternative social media applications are online avenues that offer similar functionality as mainstream platforms with more encryption and less content restriction. Examples of these platforms are Telegram, Parler, and Gab. Over the last few years, extremist-related content shared on alternative social media applications has remained constant.

In July, a federal judge sentenced Boogaloo Bois member, John Subleski, to five months in jail and a three-year supervised release for inciting a riot in Louisville. On January 5, 2021, Subleski posted to his Facebook account: "The only thing that has ever beaten tyranny was a sword or a rifles…DASSSSS IT. NOTHING ELSE! GETCHO RIFLE AND LET IT BANG AGAINST THE GOVERNMENT." He also used an encrypted messaging platform to talk with other Boogaloo Bois members participating in the riot the day of the event. He posted, "Holy s--t woman shot in capital. Ya'll lets storm [Louisville Metro Police Department]." Subleski incited protesters, provided armed security, and fired his weapon at a motorist.

Rioters assault police officers at the U.S. Capitol insurrection on January 6, 2021

Twitter joined several mainstream social media platforms in July in banning the host of a WRME podcast for violating content policies stemming from anti-Semitic and racist comments. The host rehomed the podcast to an alternative platform that also eventually banned them following the U.S. Capitol insurrection. Despite these bans, the host has maintained a support base across a variety of alternative platforms where they continue to operate.

In November 2020, California residents Daniel Rodriguez and Edward Badalian created a Telegram channel to protest the results of the 2020 Presidential election. While the channel initially started as a discussion forum, it quickly shifted to advocating for violence against groups with opposing views and promoting attendance at the "Stop the Steal" rally on January 6, 2021. According to federal authorities, Badalian posted, "we need to violently remove traitors and…rapidly replace them with able bodied Patriots." Separately, Rodriguez wrote that he would "assassinate Joe Biden" if he got the chance because he "would rather die than live under a Biden administration." Several users of this Telegram channel actively participated in the riots and brought weapons and tactical gear. Authorities arrested Rodriguez in March for assaulting a District of Columbia police officer at the rally and Badalian in November for lesser offenses related to the rally.

Targeted Social Media Content

Social media platforms use algorithms or code designed to "target" content to a specific user. Algorithms work to provide users with similar content that they have viewed or interacted with by either "liking," "commenting," or "following" accounts or posts. They can also be based on demographic and behavioral data, like age ranges or specific life events. The collected data assists advertisers in promoting their products and keeps users engaged on a specific social media platform, such as Facebook, TikTok, or Twitter.

NJ Office of Homeland Security and Preparedness

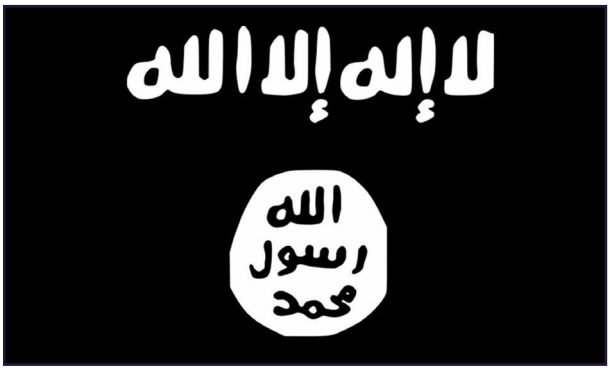
Foreign Terrorist Organizations

FTOs will likely pose a low threat to New Jersey; however, they remain dedicated to combating the United States, as well as exploiting global events to encourage homegrown violent extremists to bring the fight to the Homeland or support efforts overseas. Al-Qa'ida and ISIS have had little success in directly attacking the United States since September 11, 2001, but they remain committed to striking the nation's interests abroad and inspiring domestic supporters.

In November, al-Qa'ida in the Arabian Peninsula leader Khalid bin Umar Batarfi released a video in which he stated that the United States continues to be al-Qa'ida's top adversary as "the No. 1 enemy of Islam." In April, al-Qa'ida used the U.S. withdrawal from Afghanistan as an opportunity to display victories and smear the United States, stating that "war against the U.S. will be continuing on all other fronts unless they are expelled from the rest of the Islamic world."

Khalid bin Umar Batarfi

In January 2021, a pro-al-Qa'ida online publication called for supporters to conduct attacks in the West during recent civil unrest. The publication found the protests and riots "a unique opportunity" to conduct attacks targeting civilians or law enforcement in the United States. In July, an ISIS-aligned media group touted the spread of propaganda and influence through an "intellectual invasion" via social media targeting supporters unable to travel. The group claimed this method will result in more attacks.



ISIS Flag

In October, al-Qa'ida released an official video addressing the American people that claimed future attacks may look different from 9/11. Instead, attacks could "be more powerful, painful, and heartbreaking." Al-Qa'ida claimed that supporters are "not limited to borders and that they can move from any part of the world to execute what they wish" to deter Western oppression. In September, ISIS urged supporters in its newspaper, *al-Naba*, to "continue your incitement," encouraging attacks online and alleging that supporters' rhetoric has inspired lone wolf attacks in America.

FTOs Exploit January 6 U.S. Capitol Insurrection

In January 2021, ISIS alleged that "America would be more focused on domestic issues than those in the Middle East," making it an easier target, and that "now the time for fighting has come" in its digital weekly newspaper, *al-Naba*.

In April, al-Qa'ida commented on the events of January 6 in its English-language propaganda magazine, *One Ummah*. The group claimed the U.S. Capitol riots were evidence of a "decaying America" and urged those in the West to leave the "sunken America" for the "rescue ship of Islam."

NJ Office of Homeland Security and Preparedness

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 2021, cyber attacks affected organizations, governments, businesses, and private citizens in New Jersey. Ransomware, credential theft, and social engineering remained top cyber threats, with many attacks highlighting supply chain issues and interdependencies that increase the vulnerability of these attacks.

Ransomware

Based on public and incident reporting to the NJCCIC, there were over 3,100 ransomware incidents in 2021. High-profile and high-impact attacks at Colonial Pipeline and JBS Foods highlighted the cascading effects that could be sustained due to attacks on critical infrastructure, which were already experiencing strains to the supply chain from the COVID-19 pandemic. Also, ransomware attacks victimized many small and medium-sized businesses (SMBs), further challenging their ability to operate amid shutdowns and staffing shortages.

The average ransom demand during the third quarter of 2021 was about $140,000; however, the overall cost of a ransomware incident far exceeds that figure—often even when a ransom demand is not paid. Scripps Health, a nonprofit operating five hospitals and 19 outpatient facilities in California, was the victim of a ransomware attack in May 2021. The attack forced the health system to divert patients to other hospitals and took four weeks to fully recover from the incident. While response and recovery costs totaled $21.1 million, the cost of downtime and lost revenue during recovery efforts totaled $91.6 million. Scripps Health had a cyber insurance policy, though it was only covered for up to $20 million. The losses incurred from the attack shed light on what the actual impacts may be to victims; compounding costs of recovery efforts following cyber incidents can be particularly damaging to SMBs with slimmer profit margins or high operating costs.

Geopolitical Cyber Threats

The inapplicability of national borders in cyberspace, the commoditization of offensive cyber weapons, a hyper-connected world with an increasingly vulnerable attack surface, and heightened geopolitical unrest are ingredients that exacerbate the likelihood that nation-state or state-supported threat activity will have adverse direct or indirect impacts on New Jersey. As cyber attacks are not constrained by geographic boundaries, attacks launched against systems in geographic areas outside New Jersey may have collateral effects that threaten or impact individuals and institutions in the State.

In general, 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 criminals and 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 then carrying out their main 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 posture of the State of New Jersey and, more broadly, the United States.

CREDENTIAL COMPROMISE

Account credentials, otherwise known as the "Keys to the Kingdom," provide threat actors further network access or the ability to launch subsequent cyber attacks when compromised.

The average person has over 100 online accounts and often reuses passwords across accounts. Password managers can assist with creating and storing strong, unique passwords for each account.

Multifactor authentication (MFA) is also one of the best methods to increase account security. Choosing an authentication application or hardware token for the second factor is highly recommended. MFA can greatly reduce the risk of compromised accounts via credential theft or exposure. For example, threat actors responsible for the Colonial Pipeline ransomware incident gained network access via a user account without MFA enabled by entering an exposed password also used for a separate online account.

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 (BEC), vishing (voice phishing), and smishing (SMS-text phishing).

Social engineering campaigns carried out on social media platforms increased in 2021 based on reporting to the NJCCIC, leaving legitimate account holders without access and their contacts as the targets of subsequent social engineering attacks. Private citizens and businesses alike 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.

On December 10, Apache released information related to a critical vulnerability in Log4j, an open source logging framework developers use to keep a record of activity within an application. The flaw, dubbed Log4Shell, left countless products and services vulnerable to threat actors through ransomware, cryptocurrency mining, and other malicious cyber activity.

While a patch and mitigations were available to address Log4Shell, exploiting the vulnerability is trivial and many companies needed to spend valuable time inventorying their networks to simply determine which of their products needed updating.

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 clients.

An entity may need to adjust its understanding of its overall cyber risk to incorporate variables for these dependencies.

NJ Office of Homeland Security and Preparedness

Critical Infrastructure Protection

Foreign actors will likely commit theft, cyber intrusions, and talent recruitment to steal intellectual property from or otherwise negatively impact private-sector entities. New Jersey is home to 16 Fortune 500 companies and many other large industries driving the State's economy, including pharmaceuticals and life sciences, financial services, advanced manufacturing, information technology, and transportation and logistics. NJOHSP maintains several resources for private-sector partners to better secure their data and mitigate risks against vulnerabilities.

On February 27, 2020, a federal judge sentenced Hongjin Tan, a former employee of an Oklahoma-based petroleum company, to 24 months in prison and to pay restitution to the company for attempting to sell proprietary data to the People's Republic of China. From 2017 to 2018, Tan stole an estimated $1 billion in trade secrets and attempted to leverage the information in exchange for employment overseas with a rival company in China, according to the FBI. Federal agents found Tan accessed sensitive documents that dealt with innovative technology but did not directly relate to his work.

In November, the U.S. Department of Justice (DOJ) charged several foreign-based actors with conspiracy to commit fraud and related activity, damage to protected computers, and conspiracy to commit money laundering. According to the U.S. Department of the Treasury, the subjects victimized nine U.S. companies with ransomware. As a result of the ransomware attacks, a New Jersey-based business suffered significant disruption, resulting in compromised customer data. These charges followed a separate announcement in June, when the DOJ recovered $2.3 million in ransoms paid to an Eastern European-based ransomware group called DarkSide. The ransomware attack forced Colonial Pipeline to temporarily shut down, causing panic-driven price increases on the East Coast.

On November 4, the DOJ indicted Peter Kim, a former employee of global technology center Broadcom, with theft of trade secrets. According to the indictment, Kim stole proprietary data from Broadcom that was associated with networking chips often used in high-volume data centers. Only authorized employees could access the restricted data stored in nonpublic document repositories. Following his departure from Broadcom, Kim began working as a director for a China-based startup company focused on chip design and the market for networking chips. During the first nine months at the new company, Kim possessed and repeatedly used Broadcom trade secrets on the new company's network and other electronic devices.

PEOPLE'S REPUBLIC OF CHINA'S COUNTERINTELLIGENCE INVESTIGATIONS

On February 1, FBI Director Christopher Wray discussed during a televised interview that the FBI opens an average of two counterintelligence investigations a day as a result of the People's Republic of China spying on the United States. Wray said the investigations are not "based on race or ethnicity or constitutionally protected activity." These measures help protect targeted populations, such as Chinese Americans, from being victims of espionage or other acts of malicious intent toward the United States. Wray stated, "There is no country that presents a broader, more severe threat to our innovation, our ideas, and our economic security than China does."

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. An organization identifies, controls, and protects critical information and analyzes friendly actions and indicators that would allow adversaries or potential adversaries to identify and exploit vulnerabilities.

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.

OPSEC and Intellectual Property Protection

Domestic and foreign companies may try to illegally acquire a company's information. Foreign nations that seek to improve their economies and militaries target U.S. technology companies and others. Employing a strong OPSEC and insider threat program helps protect a company's intellectual property.

New Jersey Shield is a collaboration between the New Jersey Office of Homeland Security and Preparedness and the New Jersey Regional Operation and Intelligence Center. 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 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 webpage at
www.njohsp.gov/newjerseyshield

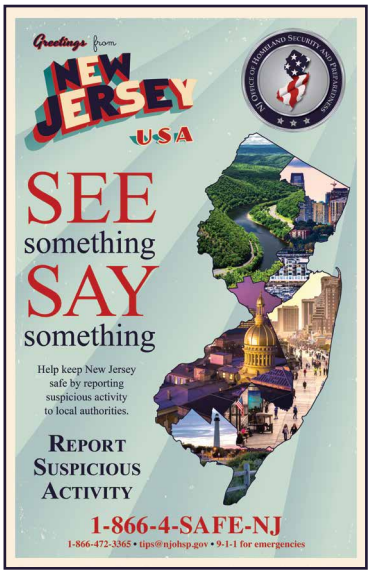
NJ Office of Homeland Security and Preparedness

SEE SOMETHING, SAY SOMETHING

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.

2022 Threat Assessment | 31

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

"Terrorism-related suspicious activity is any observed behavior reasonably indicative of pre-operational planning related to terrorism or terrorism-related crime."

U.S. Department of Homeland Security

NJ Office of Homeland Security and Preparedness

Terrorism Definitions

Al-Qa'ida (AQ) - Al-Qa'ida is 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) - AQAP is an Islamist extremist organization based in Yemen. It is al-Qa'ida's most active global affiliate.

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

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

Animal Rights Extremists - 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-Abortion Extremists - Anti-abortion extremists are individuals or groups who believe abortion is unethical and that violence is justified against people and establishments providing abortion services.

Anti-Government Extremists - 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.

Black Racially Motivated Extremists (BRMEs) - BRMEs advocate for the advancement of the black race over all others and believe that violence or criminal activity is justified to further their ideology.

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

Environmental Extremists - 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 - Hizballah is an Islamist militant group based in Lebanon and allied with Iran.

Homegrown Violent Extremists (HVEs) - 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.

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

Militia Extremists - 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.

Racially Motivated Extremists (RMEs) - RMEs advocate for the advancement of one racial or ethnic group over all others and believe that violence or criminal activity is justified to further their ideology. This includes black and white racially motived extremists.

Salafi-jihadism - Salafi-jihadism is an extreme interpretation of Islam in which individuals draw inspiration from multiple foreign terrorist organizations.

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

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

Terrorism - Terrorism is 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) - WRMEs advocate for the advancement of the white race over all others and believe that violence or criminal activity is justified to further their ideology.

NJ Office of Homeland Security and Preparedness

NJOHSP

NJCCIC

NJ SHIELD

CONTACT US

communications@njohsp.gov

njohsp.gov | cyber.nj.gov | njohsp.gov/newjerseyshield