Awareness of Preoperational Surveillance Tactics Associated With Terrorism Offers Opportunities

SCOPE: This product highlights both prevalent and novel tactics that violent extremists use to conduct preoperational surveillance as part of their attack planning. Based on observed tactics, the product offers a list of potential indicators for awareness, along with considerations and possible mitigation measures for public safety and private sector security partners.

Perpetrators of past terrorist plots and attacks have used preoperational surveillance tactics of varying complexity to facilitate their attack planning. These tactics range from physically scouting locations and note-taking to using technology—such as smart glasses or UAS—which may enhance the effectiveness of the surveillance activities while challenging detection and disruption efforts. Violent extremists may also conduct these surveillance activities themselves or use witting or unwitting surrogates, further complicating law enforcement investigations. Preoperational surveillance tactics have enabled violent extremists to choose perceived opportune and easily accessible targets, as well as to gain familiarity with locations' layouts and security posture and persons' patterns of life. Surveillance tactics may be used in combination with each other to gain an enhanced understanding of the target and its environment. Public safety personnel should maintain awareness of preoperational surveillance tactics, including how they evolve with technological innovations, to recognize suspicious behaviors and implement mitigation measures.

- On 14 May 2025, a former member of the Michigan Army National Guard and pro-ISIS individual was arrested for an alleged plot to attack the US Army's Tank-Automotive Armaments Command in Warren, Michigan. The defendant allegedly flew a UAS over the targeted facility for reconnaissance planning.
- The ISIS-inspired perpetrator of the New Year's Day 2025 vehicle-ramming attack in New Orleans used smart glasses to record as he scouted the French Quarter on a bicycle two months before the attack. ISIS messaging praised the attacker's use of the smart glasses as an example of weaponizing America's technology against it.
- In October 2024, FBI announced the arrest of two Afghan nationals residing in Oklahoma City who were connected with a plot to conduct an Election Day terrorist attack on behalf of ISIS. While it is unclear whether the attack aspirants chose a specific target, one person searched online for "How to access washington dc cameras [*as written*]" and viewed the webcams for the White House and the Washington monument, according to the criminal complaint.
- Following a failed attempt in 2021 to kidnap a US person who was an Iranian dissident, the IRGC hired members of an Eastern European criminal organization to locate, surveil, and eventually assassinate the US person. An operative repeatedly traveled to the target's neighborhood to surveil their residence and sent photographs, videos, and updates on these activities to his coconspirators abroad.

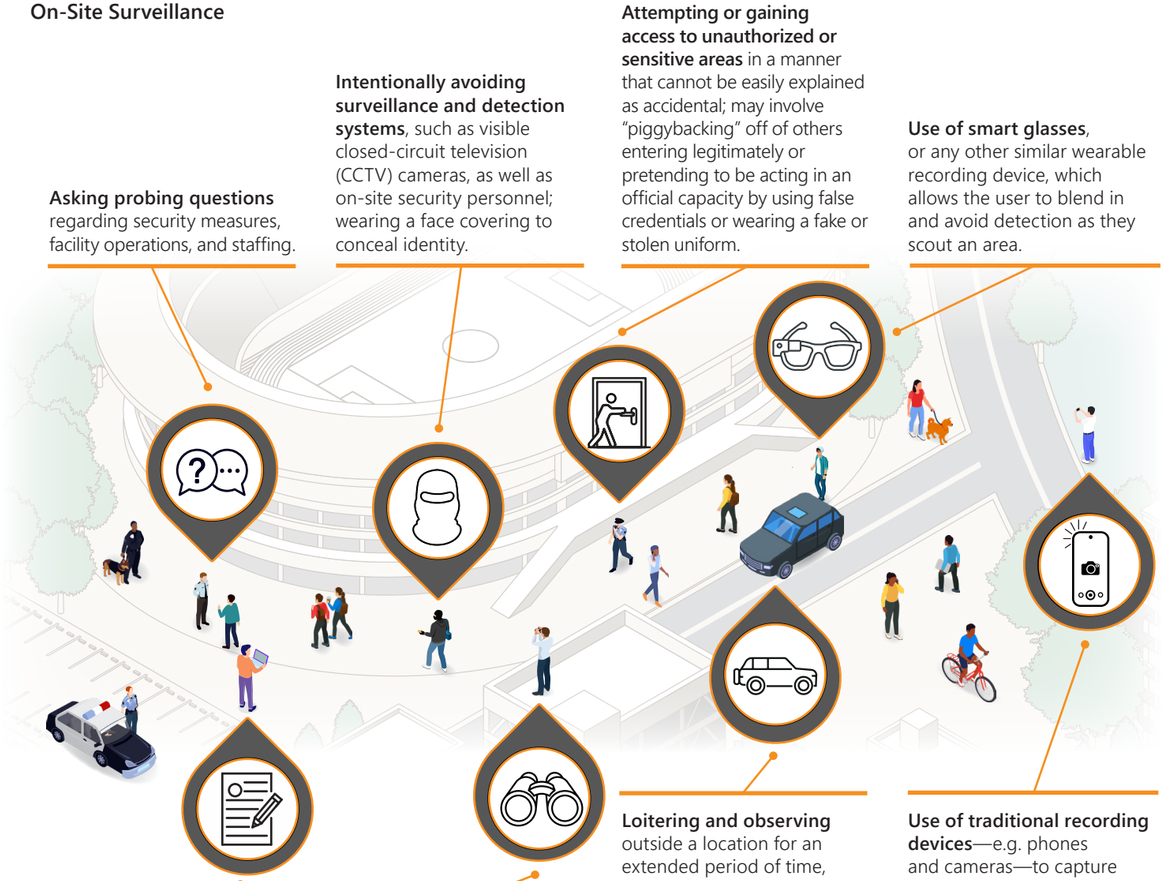
The Nationwide Suspicious Activity Reporting Initiative (NSI) includes observation/surveillance as one of its 16 indicators of preoperational planning associated with terrorism or other criminal activity. It defines observation/surveillance as "demonstrating unusual or prolonged interest in facilities, buildings, or infrastructure beyond mere casual or professional interest and in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person." According to a December 2024 National Consortium for the Study of Terrorism assessment of the NSI, observation/surveillance was observed in 31.5 percent of recorded terrorist plots from 1990 to 2022.

[a]Some of the indicators may be lawful or constitutionally protected activities under the 1st Amendment and should not serve as the sole basis for any investigative activity. Additional facts and circumstances that clearly support a determination that the observed behavior is not innocent, but rather reasonably indicative of preoperational planning associated with terrorism, are necessary to constitute a basis for reporting to authorities.

Tactics, Techniques, and Procedures (TTPs)

Potentially observable TTPs[a] that may be used to conduct preoperational surveillance of targets include on-site surveillance, target selection and attack planning, and remote reconnaissance.

On-Site Surveillance



Asking probing questions regarding security measures, facility operations, and staffing.

Intentionally avoiding surveillance and detection systems, such as visible closed-circuit television (CCTV) cameras, as well as on-site security personnel; wearing a face covering to conceal identity.

Attempting or gaining access to unauthorized or sensitive areas in a manner that cannot be easily explained as accidental; may involve "piggybacking" off of others entering legitimately or pretending to be acting in an official capacity by using false credentials or wearing a fake or stolen uniform.

Use of smart glasses, or any other similar wearable recording device, which allows the user to blend in and avoid detection as they scout an area.

Note-taking or sketching of a location, including depictions of its layout or measurements.

Unusual observation of the security response to an incident, hoax call, or exercise/drill in a manner inconsistent with the normal curiosity of a passerby.

Loitering and observing outside a location for an extended period of time, either on foot or in a parked or idling vehicle.

Use of traditional recording devices—e.g. phones and cameras—to capture entrances/exits of buildings, security checkpoints and personnel, or any other location consistent with surveillance without a reasonable alternative explanation.

NCTC-JFRT-2026-00643

12 FEBRUARY 2026
AUTHORED BY NCTC, DHS, FBI

(U) Awareness of Preoperational Surveillance Tactics Associated With Terrorism Offers Opportunities *(continued)*

Tactics, Techniques, and Procedures *(continued)*

Target Selection and Attack Planning[b]

- Choosing a Target: Attack aspirants may visit multiple locations over a prolonged period of time as they settle on a target.
- Group Deliberation: In the case of a plot involving multiple people, the group may communicate—often through encrypted messaging apps—regarding potential targets before initiating surveillance.
- Repeated Surveillance of Chosen Target: Attack aspirants may visit a chosen target on multiple occasions as they gain familiarity with the location and solidify their plans, over a period that ranges from several days to sometimes more than one year before execution.
- Surveilling an Individual: If targeting a specific person, they may surveil the target over time to establish a pattern of life and identify frequented locations, to inform their selection of a time and place for the attack.
- Third-Party Operatives: To avoid detection and attribution, highly sophisticated plotters may hire third-party operatives to scout the locations or perpetrate the act of violence.

Remote Reconnaissance

- Operating a UAS in restricted areas or densely populated locations without proper documentation or a legitimate reason.
- Viewing a publicly available online livestream or webcam associated with a landmark or other location of interest.
- Viewing a particular location frequently through online mapping applications, including satellite and street views.
- Reconstructing and exploiting a target within a virtual environment (e.g., video game or extended reality technologies) for surveillance and tactical training.

Considerations for Law Enforcement and Private Sector Security

Detecting and mitigating preoperational surveillance activity associated with terrorism can be a significant challenge for law enforcement and private sector security personnel. Often, such activity is only identified during the course of an investigation after an attack.

The following section offers considerations for implementing security measures and training aimed at identifying, preventing, and limiting the effectiveness of preoperational surveillance activities.

Security Planning

- Acquire and deploy monitoring and surveillance technology, such as CCTV systems and remote sensors and alarms. Ensure that systems are operable, monitored appropriately, and provide adequate coverage of access points and other critical areas.
- Secure nonpublic access points and conduct regular inspections. Implement an access control system, such as badging or credentialing, to enhance security.
- Consider hiring security officers who are well positioned to identify suspicious activity, respond and make notifications regarding active threats, and deter potential criminal activity.
  - Promote a culture of proactive information sharing among security officers, encouraging them to report suspicious activities even if they are uncertain whether it meets the threshold for formal reporting.
  - When appropriate, question or challenge suspicious persons present in unauthorized or nonpublic areas.
- Vary the daily routines of security officers to prevent any malicious actors from identifying patterns in security protocols, which they could exploit to avoid detection.
- Assess the security risks associated with onsite, publicly accessible webcams and consider measures to mitigate these risks.
- Regularly review, update, and exercise security plans and procedures. Consider disseminating reminders on security best practices to facility staff and stakeholders to reinforce a culture of security awareness.
- Provide regular training to security officers and facility staff on recognizing and reporting suspicious indicators and behaviors.
- Train security personnel in countersurveillance techniques to identify potential threats to the facility or staff, as appropriate.

Information Sharing and Threat Awareness

- Maintain awareness of emerging violent extremist TTPs, including those related to preoperational surveillance.
- Consider sharing real-world case studies of preoperational surveillance with community partners to enhance awareness and encourage adjustments to security procedures based on lessons learned.
- Establish procedures for reporting suspicious activity observed in and around facilities so that security staff know how to report it to local law enforcement or through methods, such as DHS's Nationwide Suspicious Activity Reporting Initiative.
  - In the event of a suspicious UAS sighting, document it with photos or videos, noting any observable modifications to the device and where it flies (e.g., near people, aircraft, or critical infrastructure). Share this information through eGuardian or using https://tips.fbi.gov/.
- Establish and maintain relationships with local commercial and retail establishments, such as hotels, office buildings, and entertainment venues, using community engagement programs to enhance information sharing and encourage suspicious activity reporting.
- Promote public messaging campaigns, such as "if you see something, say something," to encourage the reporting of suspicious activity that may otherwise go undetected.
- Engage in enhanced information-sharing opportunities available through state or local fusion centers and FBI's Joint Terrorism Task Force (JTTF).
- Maintain awareness of local or international events occurring within your area of responsibility that may necessitate an elevated security posture to enhance public safety.

Resources

DHS

- If You See Something, Say Something® is a program designed to help raise public awareness of the indicators of terrorism and terrorism-related crime. It emphasizes the importance of reporting suspicious activity to proper state and local law enforcement officials.
- The National Threat Evaluation and Reporting Office advances homeland security partner abilities to identify, investigate, assess, report, and share tips and leads linked to emerging homeland security threats. It also provides technical assistance, resources, and training associated with best practices in developing and implementing threat analysis–related activities associated with the NSI.
  - NSI
  - Assessment and Review of the NSI Indicators
- State and Local Fusion Centers are focal points for receiving, gathering, compiling, analyzing, and sharing threat-related information.

FBI

- JTTFs are composed of US law enforcement and intelligence agencies who work together and use participating agencies' resources to preempt, deter, and investigate terrorism and related illicit activities.
- eGuardian is a web-based platform where federal and state law enforcement entities can document, share, and track potential threats, suspicious activity, and cyber, counterterrorism, counterintelligence, or criminal activity with the FBI and with each other.

NCTC

- The US Violent Extremist Mobilization Indicators Booklet (2025 Edition) is an NCTC, DHS, and FBI triseal product that provides a list of observable behaviors that might help determine whether individuals are preparing to engage in violent extremist activities.
- First Responder's Toolboxes provide additional information about terrorist TTPs and considerations for response and mitigation. The toolboxes can be found on JCAT's website, DHS's Homeland Security Information Network, or FBI's Law Enforcement Enterprise Portal.
  - Reporting Suspicious Activity – Critical for Terrorism Prevention
  - Threat Assessment and Threat Management (TATM)

[b]Attackers may adjust or deviate from their initial plans at any time based on changing circumstances (e.g., hardening of selected targets, recent arrests of like-minded persons, or suspicion of law enforcement detection).

NCTC-JFRT-2026-00643

12 FEBRUARY 2026
AUTHORED BY NCTC, DHS, FBI

JCAT

JOINT COUNTERTERRORISM ASSESSMENT TEAM

PRODUCT FEEDBACK

Please use the link below to complete a short survey. Your feedback will help JCAT develop counterterrorism products that support the public safety and private sector community.

https://www.JCAT-url.com

For further information, please email JCAT
jcat@odni.gov

(U) The Joint Counterterrorism Assessment Team (JCAT) is a collaboration by NCTC, DHS, FBI, state, local, tribal, and territorial government personnel to improve information sharing and enhance public safety. The First Responder's Toolbox is an ad hoc, unclassified reference aid intended to promote counterterrorism coordination among federal, state, local, tribal, and territorial government authorities and partnerships with private sector officials in deterring, preventing, disrupting, and responding to terrorist attacks.