



Countersurveillance Guidelines

Note: This information provides an overview of countersurveillance and should not be considered all-inclusive.

What is Countersurveillance?

Countersurveillance is the process of detecting and mitigating hostile surveillance; it is an important aspect of counterterrorism and security operations. Good countersurveillance provides a means to prevent an attack from happening. Countersurveillance can be an individual or group effort, involving a dedicated countersurveillance cadre.

Representative individuals from a synagogue or school can and should conduct their own countersurveillance by being aware of their surroundings and watching for individuals or vehicles that are out of place. Once an actual attack has begun, it cannot be undone. The genie cannot be put back into the bottle.¹

How do Hostiles Perform Surveillance?

Hostile surveillance can be performed in three different forms

1. Fixed surveillance - is conducted by one or more parties that position themselves in inconspicuous locations for extended periods of time to gather information on a potential target. During this phase of surveillance terrorist operatives may disguise themselves as either security personnel, vagrants, street performers, students, photographers, utility workers, taxi drivers or any party that may easily blend into the surrounding landscape. Fixed surveillance allows operatives to document the locations of security cameras, shift changes for security and general staff, peak times of pedestrian traffic, choke points for pedestrian and vehicular traffic and other sensitive information pertaining to a potential target.²

2. Foot surveillance - is conducted by operatives that are on foot and mobile with the ability to collect information as they move from one location to another. These individuals may either pose as lost tourists or attempt to blend into nearby crowds of bystanders. Operatives may either utilize cell phone cameras, still and video photography or hand held tape recorders to gather information on a potential target site.²

3. Vehicular surveillance - is conducted by operatives that utilize various modes of transportation such as mass transit (trains, buses, ferries, aircraft etc.) automobiles and

other common vehicles. These individuals may pose as ordinary mass transit patrons and utilize cell phone cameras, still and video photography, note pads, sketch books and hand-held tape recorders to gather information on a potential target site. Operatives may often work in teams of two or more when conducting vehicular surveillance.²

Ideal locations for surveillance include areas with easy public access, multiple points of egress and views of the target site. These locations can include courtyards, bus stops, parking lots, public and semi-private roads, accessible roof tops of adjacent buildings, nearby bridges and overpasses. Adjacent wooded areas and abandon structures can also provide cover and allow views of a potential target site; these locations should be documented and routinely patrolled. An active security presence will deprive terrorist operatives of a safe haven for the collection of crucial information on a selected target.²

What Are Some Surveillance Indicators?

CAUTION: Always exercise extreme caution as individuals conducting surveillance may not only be involved in gathering information for terrorist acts but may also be involved in criminal activity. Always have available all of the telephones numbers needed to report your findings (local law enforcement, terrorism tip lines).³

Some information gatherers are highly trained individuals. One should never presume that it would be easy to identify those who may be conducting surveillance. Two common sense factors, which may help guide the counter-surveillance efforts are:

1. Frequent presence in a given area.
2. No clear or logical reason for them to be in the vicinity.

Common Indicators:

- Alone, nervous, agitated.
- Secretive, furtive behavior.
- Unusual behavior, such as staring at and quickly looking away from personnel observing them.
- Individuals waiting at a bus stop or train platform, but not boarding.
- People standing in public or customer service areas, but not requesting service.
- A person leaving a package or knapsack behind as they exit public transportation or crowded area.
- Unusual interest in security measures, equipment and/or pedestrian traffic flow.
- An unidentified individual asking questions that pertain to facility infrastructure and security measures, in person or on the phone
- Unexpected deliveries or services.
- Activity not consistent with location or task being conducted.
- Loose or bulky clothing not suited to current weather conditions.
- Unattended packages, briefcases, and other items.
- Unusual accessories not fitting in with the area or the individual (e.g., baby strollers, shopping carts, backpacks, delivery bicycles with storage compartments, ice cream carts).
- Equipment not consistent with commonly seen items within the area (e.g., Global Positioning Satellite devices, movie and still cameras, voice recording, sketching

- tools).
- Rigid, stiff midsection (indicative of concealed explosives or weapons).
 - Exposed wires or switches.
 - Hands not visible or tightly held.
 - The deliberate, cautious actions of a person handling packages, backpacks or baggage.
 - Individuals not fitting into the surrounding environment (e.g., individual wearing a winter coat in summer, a backpack, a large duffle bag, suitcase).
 - Individuals observing reaction drills, procedures, response times, and security equipment.
 - Illegally parked vehicles in and around your facility.
 - Individuals working in pairs or groups who appear near same location on multiple occasions.
 - An individual may create a scene to distract security personnel while the accomplice attempts to enter the facility.
 - Individuals conveniently getting lost or disoriented while visiting your facility.
 - Unannounced and/or unauthorized maintenance work.
 - Persons or vehicles seen in the same location on multiple occasions; an individual sitting in a parked vehicle for an extended period of time.
 - Individuals disguised as panhandlers, shoe shiners, newspaper, and food or flower vendors, not acting consistent with their tasks.
 - Individuals who do not work, have business, or belong in their current area, attempting to befriend someone to obtain sensitive information or attempting to blend in.
 - An unknown individual hands you a parcel or letter for deliver to a building or for the mail.
 - Persons observing (testing) your emergency response to abandon packages, suspicious activity, criminal activity and/or motor vehicle accidents.
 - Persons observing your emergency evacuation drills and or assembly area's.
 - Individuals who appear to be conducting surveillance (e.g., explicit or discreet use of picture taking, video cameras, cell-phone cameras, binoculars, note taking, and/or sketching) of your facility.
 - First responder vehicles or trucks being stored in unusual locations.
 - First responders who do not appear to fit in or know what to do.

If you suspect malicious surveillance, you should carefully and covertly monitor it and report this information immediately to the appropriate law enforcement authorities. Try to remember as much as possible about the individual conducting the surveillance, his or her clothing, personal identifying characteristics, their points of interest, vehicle information, and possible accomplices. It is recommended that once you have completed your observation, you retreat to a location several blocks away from the targeted location to meet with authorities. Avoid causing undue attention; never arouse interest in yourself from a possible adversary.³

What are some other indicators of Suspicious Behavior?

1. An unidentified individual observed loitering near a facility or in the lobby of a facility for an extended period of time.

2. An unidentified individual observed wandering nearby or throughout your facility.
3. An unidentified individual dressed in oversized or inappropriate clothing (e.g. - a long heavy coat in warm weather) that appears to be concealing something.
4. An unidentified individual entering a facility carrying an oversized backpack or a large suitcase.
5. An individual who, when challenged by a supervisor or an employee, does not respond or does not provide a reasonable explanation for his/her actions.
6. An unidentified individual asking specific questions about your facility (e.g., security related matters, etc. **either in person or by phone**)
7. An unidentified individual asking questions about key personnel (e.g., their normal arrival or departure times, their vehicle, location of their parking space, etc.).
8. An unidentified individual trying to deliver a package or other item to an office or to a specific person.
9. An unidentified individual observed photographing, videotaping and/or sketching the exterior or interior of your facility.
10. An individual without proper identification entering your facility claiming to be a contractor, law enforcement officer, reporter or a service technician

Sources:

- (1) Strategic Forecasting, *Vulnerabilities in the Terrorist Attack Cycle*
- (2) Stanley White, *Combating Hostile Surveillance*
- (3) Global Security Risk Management