**COUNTER SURVEILLANCE**

Regardless of how small or how big the plan, some form of surveillance occurs. Attackers will seek to exploit vulnerabilities of facilities in order to expedite planning, save resources, and to give them a better opportunity to succeed. Counter Surveillance, the process of detecting and mitigating hostile surveillance, is an important element of counter terrorism and security operations.

An effective Counter Surveillance program depends on knowing hostile surveillance is vulnerable to detection. Those performing surveillance are not always as sophisticated as commonly perceived, and second, hostile surveillance can be manipulated and the operatives forced into making errors, revealing their presence.

A large, professional surveillance team requires an organization with vast assets and well trained operatives. This level of surveillance is usually only found at the governmental level, as most militant and criminal groups lack the resources to conduct this type of surveillance. Surveillance conducted by these groups is often one person or a small group of operatives. This means they must place themselves in a position to see the target therefore can be seen. The more they show their faces, the more likely they are to be discovered.

In 2000, the Manchester, England police discovered a document which became known as “The Manchester Document.” That document was discovered to be a training manual for “jihad” against the West, non-believers, and “infidels” written by al Qaida. In the document is a section titled “Espionage.” Instruction is given in how to live among the enemy, open source information gathering, covert sources and mobile surveillance. It also describes methods for detecting counter surveillance.

While the al Qaida manual instructs operatives to conduct surveillance and what information to gather, it relies on the individual to decide how to go about gathering that information and does not offer formal training, thus resulting in untrained “spies.”

“Bad” surveillance can be recognized by poor demeanor making one look blatantly suspicious, taking obvious pictures of security devices, communicating when security personnel move, any number of items that make their presence obvious.

A dedicated Counter Surveillance team can be deployed to determine whether a person or facility is under surveillance. This team can use mobile assets, fixed assets, or a combination of both. The CS team is essentially tasked to watch for watchers.

These mistakes are easy to catch **as long as somebody is looking for them!**

**I. THE COUNTER SURVEILLANCE HIERARCHY**

The need for Counter Surveillance can be pictured in a model of hierarchy, consisting of Risk Analysis/Assessment, Vulnerability Assessment, Hostile Surveillance Assessment, and Counter Surveillance Assessment. As a Counter Surveillance Team, the mere fact you exist probably means someone has already completed a Risk Analysis and determined your area of responsibility is a potential target.

|  |
| --- |
| RISK ANALYSIS/ASSESSMENT |
| VULNERABILITY ASSESSMENT |
| HOSTILE SURVEILLANCE ASSESSMENT |
| COUNTER SURVEILLANCE ASSESSMENT |

**Risk Analysis/Assessment**

Risk Analysis is the process by which the risk potential of an asset is determined; terrorists typically pick targets for three reasons: (1) mass casualties, (2) news coverage/emotional effect, and (3) interruption of critical services. Risk Analysis determines the potential for an attack on critical infrastructure, key resources, or people. Is the asset a potential target? The chances are this has already been done for you or you would not have the job you have.

**Vulnerability Assessment**

Vulnerability Assessment is the study of a person, place, or thing (People, Critical Infrastructure, or Key Resources), to determine its’ vulnerabilities or potential areas of attack. If the asset is a potential target (risk), where is it most vulnerable and subject to attack?

**Hostile Surveillance Assessment**

Hostile Surveillance Assessment is the process of determining the Hostile Surveillance Positions from which a hostile may position themselves to observe the vulnerabilities of an asset. If the target is chosen for attack, where are the positions that Hostile Surveillance will need to position themselves to properly surveill a location.

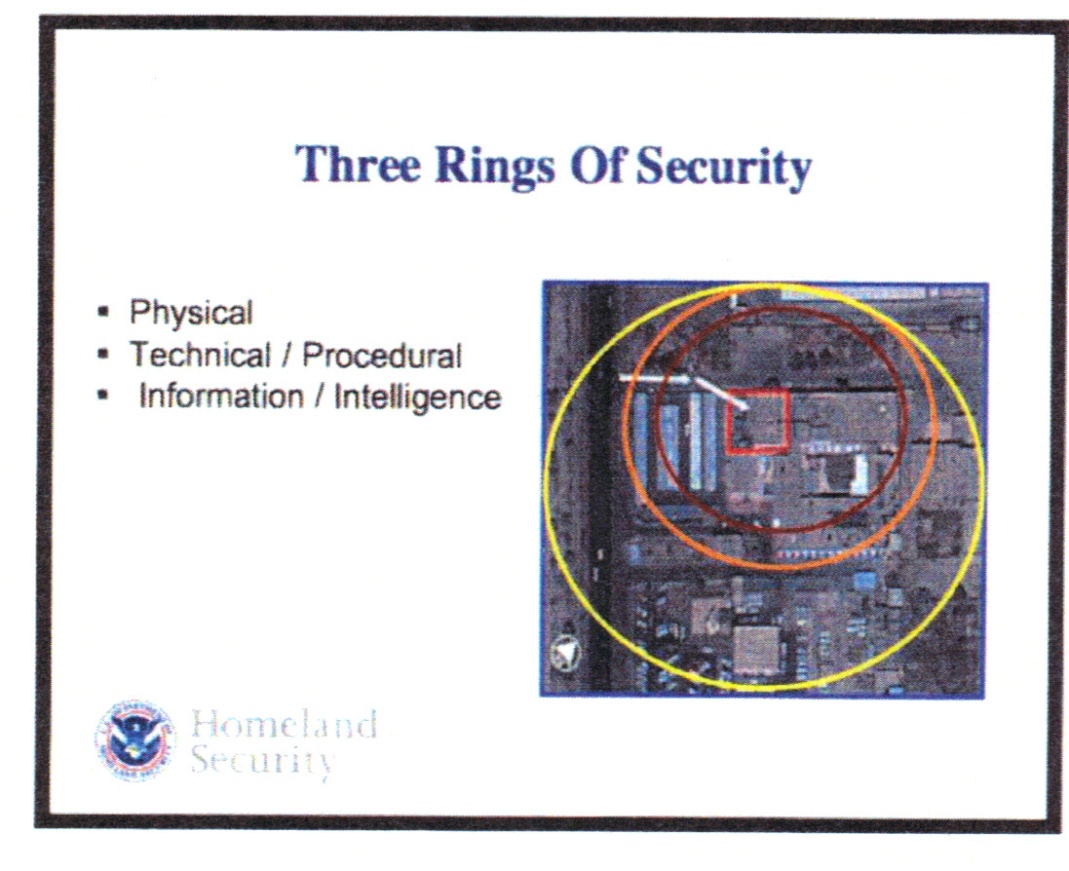
**Counter Surveillance Assessment**

Counter Surveillance Assessment is the process of determining the positions a Counter Surveillance Team needs to occupy in order to observer Hostile Surveillance Positions. What are the positions Counter Surveillance team members must occupy to see where hostile surveillance is?

While a highly trained Counter Surveillance Unit is a valuable asset in protecting critical infrastructure and people, too often, security relies upon the first two rings of security to prevent attacks.

**II. THREE RINGS OF SECURITY**

Facility security can be divided into three sections or “Rings.”



The first level of security is the **Physical** ring. This includes walls, fences, gates, guards, and landscaping. This ring is a visible ring, i.e. citizens and potential attackers can see this ring.

The second level of security is **Technical/Procedural**. This includes ID checks, entry badges, access code entry, alarm systems, CCTV, and cameras. This ring is also a visible ring.

The third security level and perhaps most important, is the **Information/Intelligence** ring. This ring provides intelligence from the outside. This is information the opposition does not know you have. This ring is **NOT VISIBLE** making it extremely important in protection and extremely difficult for an opponent to defeat. This is where Counter Surveillance operatives live and work.

**Counter Surveillance is not intended to work where physical and technical security reside, but in that world where they do not exist. Once an attacker has entered either of the first two rings, you can only hope to mitigate damage, but if you can identify the attacker before he gets to either of those rings, you can stop the attack, saving lives and property.**

**III. 7 STEPS OF THE TERRORIST PLANNING CYCLE**

In order to better understand how to use the Information Ring of security, it is necessary to understand the planning cycle in an attack.

1. Broad Target Selection
2. Intelligence and Surveillance
3. Specific Target Selection
4. Pre-attack Surveillance and Planning
5. Attack Rehearsal
6. Actions of the Objective
7. Escape and Exploitation (Depending on the nature of the attack group, this step may not be a consideration given today’s climate of suicide bombings)

The detectable events in preventing an attack occur in steps 2, 4, and 5. CS has the most time to detect hostile surveillance in these steps. During these stages, elements of an attack group are observing the vulnerabilities of a facility to help with a final target selection or fine tuning a plan on a selected target.

**IV. HOW TERRORISTS PICK TARGETS**

Targets are rarely chosen based on military or utilitarian reasons. Targets are generally chosen that have symbolic value or that will elicit the greatest media attention. One way to guarantee this is by killing and maiming a large number of people.

The purpose of pre-operational surveillance is to determine a target’s vulnerabilities. Surveillance helps to quantify the target, note possible weaknesses, and even begin to identify potential attack methodologies.

Attackers will observe the two rings of security that are visible (Physical and Technical/Procedural) in order to pick a target. For fixed targets such as buildings, surveillance will be use to determine physical security measures (the first ring) and patterns and behaviors of the security force (the second ring).

They will attempt to gain critical information about facilities, personnel, and activities in order to determine levels of awareness, predictable patterns and routines, vulnerabilities, and times, locations, and avenues of approach.

Surveillance will look for predictable patterns such as: standard workday comings and goings, regularly scheduled visitors/events, procedural practices/drills, service calls/scheduled deliveries, and regular services provided to the public such as tours.

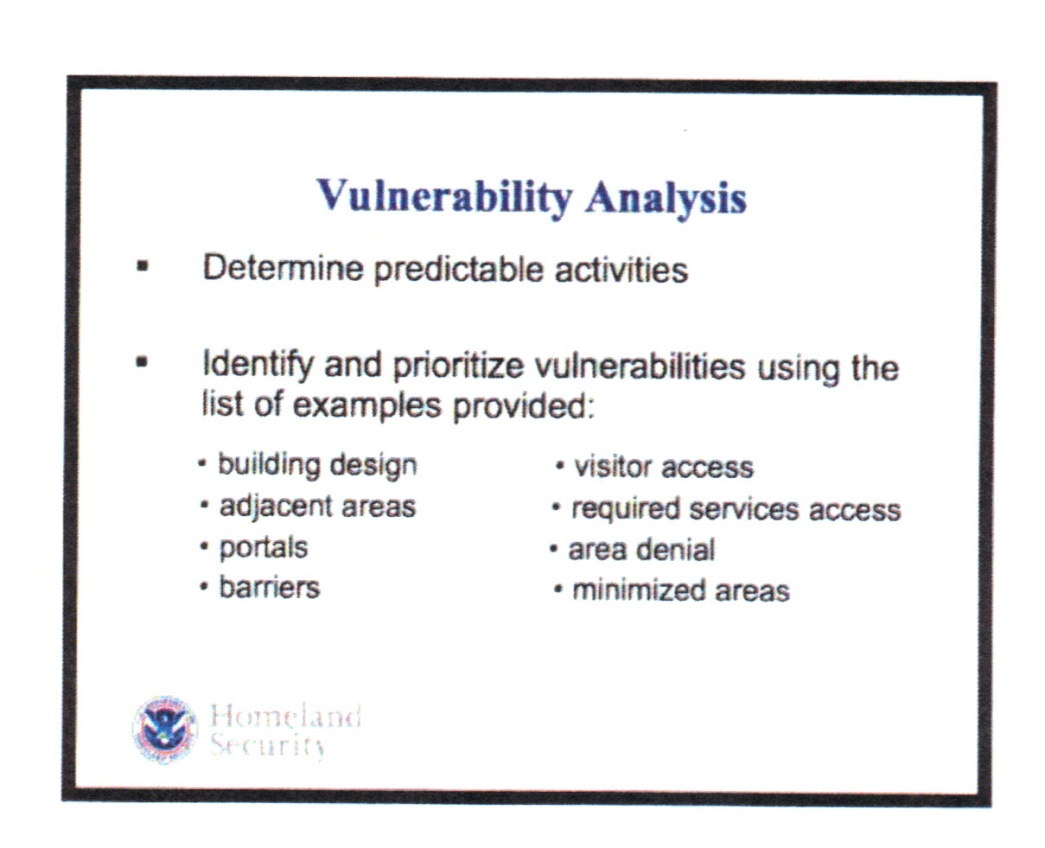
Surveillance takes time. Depending on the selected target, surveillance may take months or even years. Hostile surveillance will have contingency plans for changes in security postures that will allow for some flexibility in their planning.

Individuals selected to perform this type of surveillance will know how to position themselves to look for vulnerabilities, will possess area knowledge, and will operate with the knowledge they have more time to adjust to any changes that pose problems for their surveillance operations.

**V. VULNERABILITY ASSESSMENT**

Before Counter Surveillance can identify where hostile surveillance positions may be and where to place counter surveillance positions, a Vulnerability Assessment should be conducted.

A Vulnerability Assessment is the method used to determine a facility’s vulnerable areas for attack as well as predictable activity surrounding the facility.

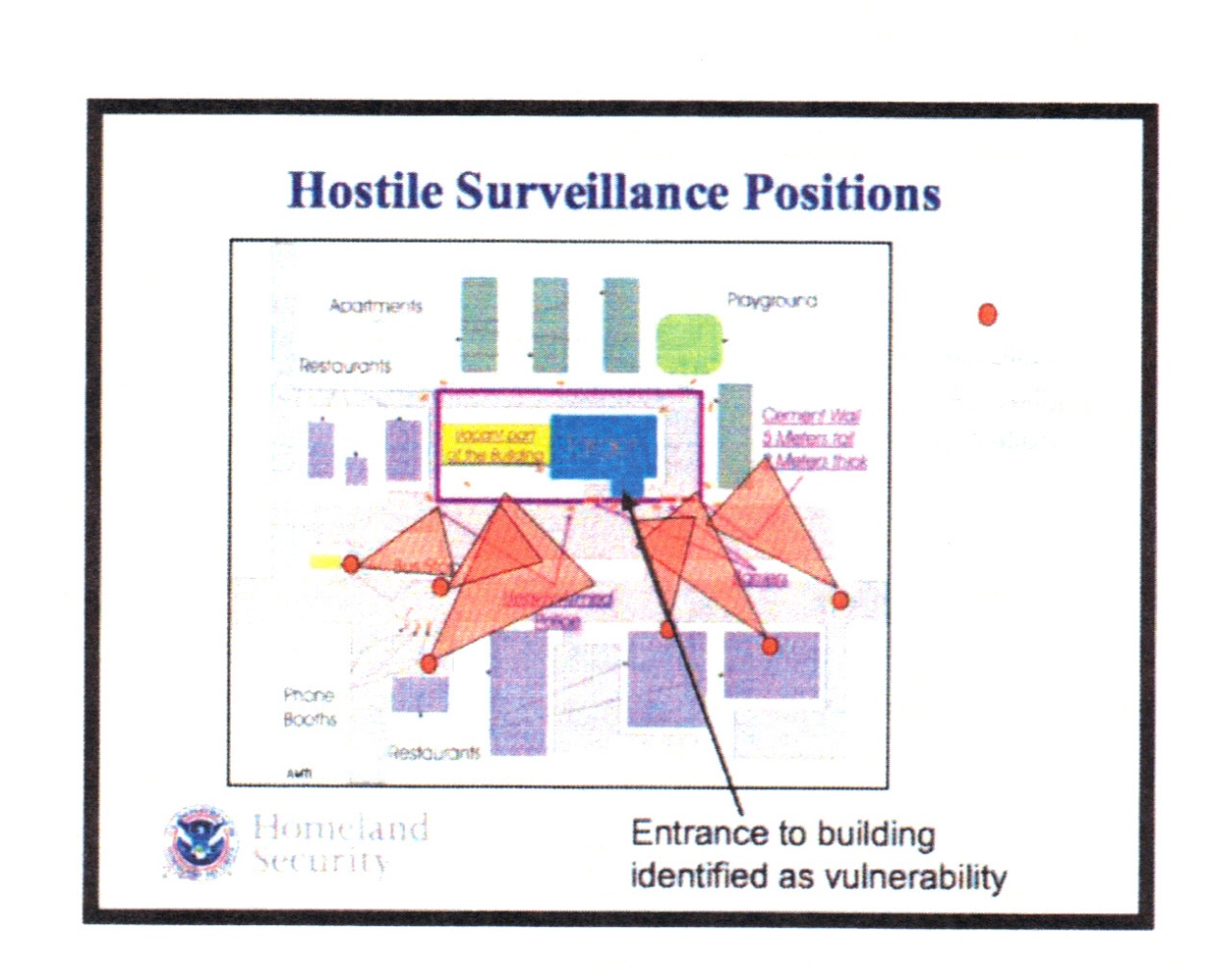


It is necessary to view the facility and its weaknesses from the perspective of the attacker, **from the outside looking in**, rather than that of currently existing security plans or procedures (inside looking out) in order to anticipate the attackers’ potential actions.

Observing the vulnerabilities from the **“outside looking in”** helps security better prepare to see the situation as the attackers would, detect hostile surveillance, anticipate terrorist activities, and could ultimately thwart the terrorists’ plans to attack a facility.

**VI. HOSTILE SURVEILLANCE POSITIONS**

Given that Hostile Surveillance Positions are specific points surveillance should occupy to view the vulnerability, the determination of the locations of these points is an extremely important part of any Counter Surveillance Plan.



To accomplish this, the Counter Surveillance team must conduct Vulnerability Assessment, study the area, and recognize certain factors about particular positions around the facility’s vulnerability.

In conducting the Vulnerability Assessment, the team must be objective and realistic in identifying all the vulnerabilities and activities surrounding the vulnerabilities.

Area knowledge is important to the Counter Surveillance team as they will be operating in the environment with the hostile elements. Characteristics of the area will dictate the racial, ethnic, and gender make-up of the hostile surveillance team and may be a consideration of the Counter Surveillance team as well.

**VII. COUNTER SURVEILLANCE FUNDAMENTALS**

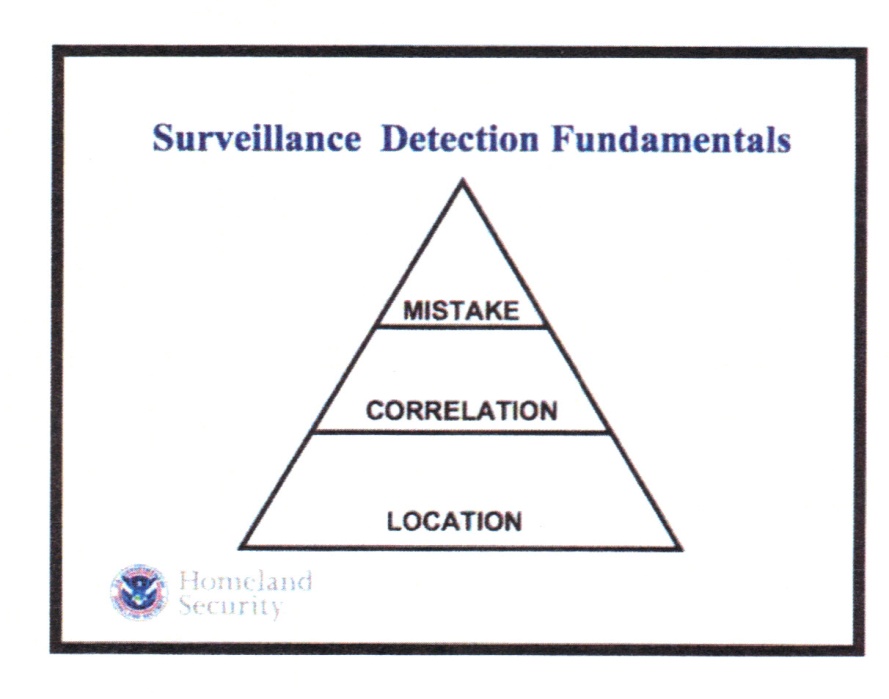
Counter Surveillance team members must know where the attackers will need to be to see a target’s vulnerabilities. In-depth analysis of facilities and surrounding areas in conjunction with the operational planning is absolutely critical to the operational effectiveness of any Counter Surveillance team. This analysis enables Counter Surveillance team members to determine where to position themselves.

Counter Surveillance needs a view of hostile surveillance positions. **IT DOES NOT REQUIRE A VIEW OF THE TARGET!**

CS requires:

* A view of Hostile Surveillance Points
* Cover/Concealment
* Entry/Exit

**The Counter Surveillance Pyramid**



**Location**

* Location includes the areas of the facility identified during analysis as being likely surveillance locations allowing observation of the target and specifically the vulnerabilities of the target.

**Correlation**

* Correlation is any activity directly related to the facility including repeated sightings of individuals correlating with the facility or vulnerability.

**Mistake**

* A mistake is something that occurs when Hostile Surveillance inadvertently exposes its presence. Mistakes can result from bad surveillance abilities and/or poorly developed cover. Do not depend on Hostile Surveillance to make a mistake to verify its presence.

If you see a person at a **location** that has been identified as vulnerability, if you **correlate** activity from the same person repeatedly, and if that person makes a **mistake** such as being observed taking inappropriate pictures, then there is a reasonable chance hostile surveillance is occurring and you need to proceed with further investigation.

In the past, the federal government has taught the acronym **TEDD**, which can also be used like the Counter Surveillance Pyramid. If you see someone repeatedly over **T**ime, in different **E**nvironments, acting with different **D**emeanors, and over different **D**istances, they may be worth a closer look.

**VIII. RECOGNIZING SURVEILLANCE TECHNIQUES**

Most experts recognize surveillance conducted by untrained groups is unsophisticated at best. However, even those without professional training are trained to conduct their business with an eye towards thwarting discovery of their presence and purpose.

A Counter Surveillance member can use Surveillance Detection Routes to recognize certain behaviors from suspected hostile surveillance operatives.

* **The Channel**: The channel is any long straight corridor that has exits at the far end but not in the channel itself. Areas such as hallways, pedestrian or vehicle bridges prevent an effective parallel track from being conducted.
* **The U-turn**: Any movement where a person suddenly reverses direction with the purpose of determining if they are being followed.
* **The Stair Step:** Stair-stepping involves making turns that deviate slightly from a direct route. These types of movements require a multi-person team to defeat.
* **Intrusion Point:** An intrusion point is any place where a hostile surveillant can stop, preferably with a back exit. This is usually some type of public place such as a restaurant. When a hostile surveillant enters a public place, there is the risk of an exit out the back.
* **Timing Stops:** Timing stops involve temporary stops to look around for surveillance. It doesn’t require a long period, just enough to ascertain if he is being followed.

Any of these Surveillance Detection Routes can be confirmation of hostile surveillance. A well trained Counter Surveillance team will recognize these techniques and use them to their advantage when following or "tracking" a subject. Remember, this can be difficult, because all your counter surveillance moves must appear as ordinary behavior for your team to be successful.

**IX. BEHAVIOR PATTERNS**

Learning the behavior patterns, hostile surveillants will use is a strong tool in the Counter Surveillance agents’ arsenal. Counter Surveillance agents will be able to:

* Help identify the "bad guys" trying to commit a terrorist act or trying to gather information
* Allow agents to recognize unusual and out of the ordinary in a subject's behavior and to focus on the exhibited signs.
* Analyze suspicious behavior and patterns to decide whether to act.

Behavior pattern indicators are numerous, but some of the more common are:

* **Observation/Surveillance**: demonstrating unusual interest in facilities, buildings, or infrastructure beyond mere casual or professional interest such that a reasonable person would consider the activity suspicious. Examples include observation through binoculars, taking notes, attempting to measure distance, etc.
* **Photography**: taking pictures or video of facilities, buildings, or infrastructure in a manner that would arouse suspicion in a reasonable person. Examples include taking pictures or video of infrequently used access point, personnel performing security functions, security related equipment, etc.
* **Testing Security**: Interactions with, or challenges to installations, personnel, or systems that reveal physical personnel or cyber security capabilities.
* **Eliciting Information**: questioning individuals (guards, Officers, employees) at a level beyond mere curiosity about particular facets of a facility or building's purpose, operations, security procedures, etc, that would arouse suspicion in a reasonable person.
* **Mannerisms**: An act or function that is a normal activity, but conducted with other motives. A subject reading a newspaper or book, who spends more time looking than reading, or standing on a corner longer than everyone else, are examples of mannerisms that may be behavioral indicators.

**X. COUNTER SURVEILLANCE TACTICS**

Ideally, any track of a subject should be a team effort. The more team members, the easier to avoid detection, but some of the tactics can be used by small group or individual members.

* **The Eye**: Having the "Eye" means the team member who actually has visual contact with the subject. It is good practice to pass the eye as often as practical to help avoid being observed by the subject.
* **Parallel Track**: In an individual member track, this is as simple as following on the opposite side of the street. In a team track, this will include having a team member a block over on either side of the subject.
* **The Box**: The team disperses around the subject in the shape of a box and moves with the subject keeping him in the middle of the box.

By following these tactics, the team or an individual agent should be able to follow a subject to a final destination where additional information can then be obtained, address, vehicle license plate, etc.

**Subject Observation**

When observing a subject, keep in mind Behavior Patterns. When a subject conducts himself in a manner to raise your suspicion level, it is time to call in someone who can make a consensual contact and perhaps identify the subject.

**AGENT CONTACT WITH A SUBJECT SHOULD ONLY HAPPEN AS A LAST RESORT!**

**Cover**

The developing of cover requires area knowledge and should give anyone looking at the individual an instant answer as to why that person is there. Cover creates a logical reason for someone to be in a certain area while operation as a Counter Surveillance team member. Think it through and don’t choose cover that will distract you from what you need to do. Recognize that Hostile Surveillance will use cover as well.

**Developing Cover**

Counter Surveillance must know what normally happens and what belongs in the area. This requires research. A Counter Surveillance team member must determine what normal activities and behaviors could be effective cover. Not all cover will work for all team members. Determine who can use certain cover when, where, and how often. Counter Surveillance members must maintain cover at all times while in the operational area.

* Counter Surveillance must know what happens and what normally belongs in the area. This requires research.
* Determine which of the identified “normal” activities or behaviors could be effective cover for Counter Surveillance team members and for how long.
* Chose cover keeping in mind not every cover will be appropriate for every team member. Determine who can use certain cover when, where, and how often.
* Developing cover is a team effort. Placing too many homeless people at an intersection could be overkill and a giveaway.
* Discuss communications needs. A bunch of people with Blackberry's is another giveaway.
* Maintain cover at all times while in the operational area.



Cover does not need to be elaborate to be effective. As these examples show, knowing the area you are working in and dressing according to the area is the most effective cover.



The use of props (dog, guitar) can add to the appearance of fitting in.

It is important that whatever cover is chosen blends with the area and the conditions. Not all cover will be appropriate.



**XI. WORKING COUNTER SURVEILLANCE**

Counter Surveillance is not for everyone. It is a big picture job and there is rarely a point of instant gratification as in, say, a DWI arrest. Chances are slim you will ever be recognized for what you do. Anonymity is your friend and keeps you safe. Anonymity also protects your team. If you are discovered or suspected, then anyone you associate with becomes suspect, such as your team members. You have to decide if that is a risk you need to take for a quick contact with a subject. Remember, a terrorist is someone who wants to kill you, the reason is irrelevant.

Victims of crime all have one thing in common, none of them asked to be victims. Whether it is a purse snatching victim or a suicide bomber casualty, none of them asked to be assaulted. In the field of Counter Surveillance, you have an opportunity to stop crime before it happens, whether it is by facilitating an arrest or just running someone off to another target. For the Counter Surveillance agent to have a successful day, it is not necessary for anyone to be arrested. If you make the hostiles think, "This is too hard. I'm going someplace else." then that's a good day. At the end of the day, you go home knowing you saved lives.

Perhaps STRATFOR Global Intelligence said it best, "Anti-terrorism experts who say the key is not to be able to run faster than the bear, just faster that the other person, are right on target."

**SOURCES**

**1.** "**The Secrets of Countersurveillance"**, Fred Burton, STRATFOR Global Intelligence, June 6, 2007

**2. "Surveillance Detection Training"**, Department of Homeland Security

**3. "Surveillance/Countersurveillance"**, Barry Eisler, December 17, 2009

**4. "Countersurveillance-'Who's Watching You Now?'**, Chuck Tobin, AT-RISK Protection and Investigations.

**5. "The Terrorist Attack Cycle: Selecting the Target,"** STRATFOR Global Intelligence, September 30, 2005.

**6. "Behavior Pattern Recognition,"** Ann Mary Murphy, MAYDAY International