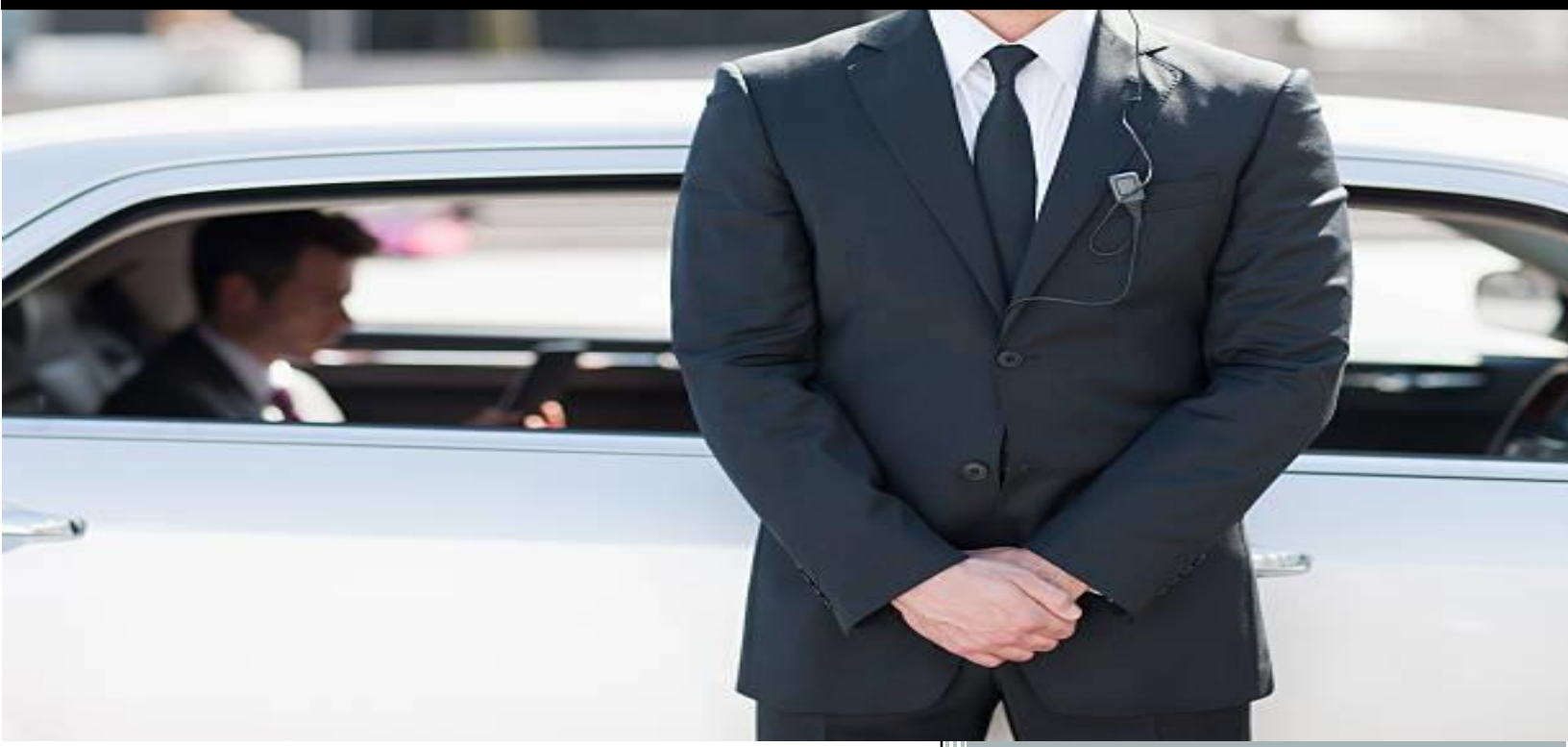
# *Surveillance Detection & Avoidance for Executives & Protection Specialists In High Threat Environments*



**Gerald L. DeSalvo**

**Managing Director**
**Wellington**
**Global Security Group**

**2018**

## About the Author

**Gerald L. DeSalvo, Managing Director,** of **The Wellington Global Security Group,** is an international management and training consultant specializing in law enforcement and security issues.

He has more than 40 years of operational, managerial and senior executive experience in U.S. federal law enforcement/investigations/security, municipal policing, military intelligence, training program administration, and management of international police training/assistance programs. His international experience includes 15 years living and working in Latin America, Asia, and Europe.

Mr. DeSalvo has extensive international managerial experience in the following areas: security management; criminal investigations; executive protection; threat analysis; security risk management; facility protection; anti-terrorism operations and planning; guard force management (including a 600-person armed guard force); training development & instruction; international police liaison; emergency planning; crisis management; crime prevention planning; the development of comprehensive policies, plans and procedures; contract management; special event security planning; Central Station management; and security and law enforcement training academy administration.

He has two graduate degrees. A master's in Criminal Justice Administration and a second in Liberal Studies (with a research emphasis in Training & Development). He also completed extensive graduate study in business administration and human performance improvement.

# SURVEILLANCE DETECTION AND AVOIDANCE FOR EXECUTIVES & PROTECTION SPECIALISTS *IN HIGH THREAT ENVIRONMENTS*

It is well known in executive protection circles that both criminals and terrorists use surveillance of potential targets in their planning for kidnappings, extortions and assassinations. The Office of the Director of National Intelligence's, "Terrorist Attack Planning Cycle" shows that terrorists use surveillance in two stages of their attack planning: the initial phase and the pre-attack phase.

The information developed in these surveillance activities allows the attackers to decide which target offers the best probability for a successful attack. Typically, the attackers are looking for: (a) information on the ease of access to the potential target, (b) the level of security provided to the target at their place of business, residence, and other places frequented on a regular basis [e.g., church, health club], (c) the level of security awareness exhibited by the target, (d) the level of physical protection provided to the target in the form of bodyguards, armored cars, police support, etc., and, (e) the chance for a successful escape from the attack scene [not applicable to suicide attacks]. So, what are some of the criminal and terrorist (***C/T's***) surveillance methods?

ODNI - Terrorist Attack Planning Cycle

1. PRELIMINARY TARGET SELECTION
2. INITIAL SURVEILLANCE
3. FINAL TARGET SELECTION
4. PRE-ATTACK SURVEILLANCE
5. PLANNING
6. REHEARSAL
7. EXECUTION
8. ESCAPE & EXPLOITATION

## The Four Primary Criminal and Terrorist Surveillance Methods

The four principal methods of surveillance used by ***C/T's*** are:

1. **Fixed position surveillance**
2. **Vehicle surveillance**
3. **Foot surveillance**
4. **Technical/Signal surveillance**

Let's briefly examine each of these four methods.

**Fixed Position Surveillance**

Many times, ***C/T's*** use a fixed position surveillance to begin their information gathering on a potential target. They typically begin their fixed position surveillances at a potential target's business/work location. If they are looking, for example, for the chief executive or country manager of an organization, one of the easiest locations to begin their surveillance on the target would be at the main work site of the business or organization.

The **C/T's** will undertake their surveillance activities in the most discreet manner possible based on local conditions. They will normally dress in inconspicuous clothing, appropriate for the location under surveillance, and engage in normal activities for the surveillance location [e.g., eating breakfast in a restaurant or food stall in front of the work location, buying a newspaper in front of the location, waiting for a bus or taxi at a stop across the street from the location

under surveillance]. How they conduct a discreet surveillance at the potential target's work site is only limited by the imaginations of the ***C/T's***.

Some of the information they will look for at the target's work location is described below.

They will be looking for any distinguishing characteristics about the vehicle that indicate the potential target is inside, such as: special license tags, a special type of vehicle [e.g., black limousine – typically used by the company's executives or motor pool], special vehicle characteristics [e.g., darkly tinted windows or curtains, does it appear to be an armored vehicle], information on the driver – is the vehicle being driven by the potential target or is a chauffeur driving, and finally does it appear that there are security personnel in the vehicle.

At the work location, the ***C/T's*** will typically arrive at their fixed position surveillance locations sometime before normal working hours begin at the site to observe what time the potential target arrives at the work location and how (e.g., what entrance does he/she use, where do they park, etc.).

If a security team is present, they will note the security procedures used by the team when the potential target arrives at the work location. For example, they will be looking to see if the potential target is dropped off by him/herself at the curb in front of the work location while the driver departs and parks the vehicle.

If the target is accompanied by a security escort, does the escort accompany the potential target inside the building or does the security escort wait outside while the potential target enters the building. They will also note if there is a visible security presence at the arrival point when the target arrives at, and departs from, the building (advance security personnel). They will also count the number of security personnel

and note whether they are armed. If armed, they will try to determine what type of firearms they are carrying.

They will then repeat this process in the afternoon (lunch time) and closing hours of the business or work location.

**Vehicle Surveillance**

Once the potential target's vehicle has been clearly identified at the work location, and his/her normal arrival and departure patterns have been established, the ***C/T's*** will frequently attempt to establish a vehicle surveillance of the potential target starting at the business or work location (initially at the end of a typical work day). By starting their vehicle surveillance at the business or work location, at the end of the work day, they can follow the potential target to their residence, or other location that they regularly visit after work, before going home [e.g., gym, church, children's school]. *It should be noted that, kidnappings and assassination attempts on Executives while in transit are two of the most popular attack scenarios.*

Once the potential target's residence has been located, the ***C/T's*** can begin a surveillance at the target's residence in the mornings, at approximately the time the potential target would depart their home for their work location. This residential surveillance could begin with either a fixed or vehicle surveillance.

When the potential target's vehicle, and arrival and departure time routines have been discovered, they would use a vehicle surveillance to determine the *routes* the potential target uses *to and from* his/her work location. They could also begin a surveillance at the potential target's residence to determine its

security posture. In addition, they would study the daily routines of the target's family, and his/her routine after working hours and on weekends.

The vehicle surveillance could be undertaken by one or more vehicles. The ***C/T's*** will normally use vehicles that are inconspicuous and appropriate to the area where the surveillance begins. These vehicles could be regular sedans, trucks, taxis or motorcycles. In residential areas where the ***C/T's*** vehicles might be noticed, they may begin their vehicle surveillance several blocks from the residence at a more discreet location along the route normally taken by the target *to and from* work. They could then begin their vehicle surveillance from a better, less obvious location, thereby reducing the chance of being detected by the target.

While conducting their vehicle surveillance the ***C/T's*** will also be looking for the routes the potential target uses to and from work, and to and from regularly visited locations. They will attempt to locate vulnerable points along the routes such as, choke points (e.g., locations where traffic narrows, slows or stops, overpasses, road construction, one-way streets) where an attack can be undertaken under the most advantageous conditions for them.

**Foot Surveillance**

The next method that is used by ***C/T's*** to conduct a surveillance of a potential target is foot surveillance. This could be conducted by one or more ***C/T's*** who will try and blend in to the local environment while conducting their surveillance. A typical foot surveillance might be initiated from a fixed surveillance position in front of an office building and begin at lunchtime if it is determined that the potential target goes out on foot every day at approximately the same time for lunch. It might also be used to gather information on the security in place at an office building or parking garage frequented by the target, with the ***C/T's*** posing as normal customers or visitors to the location. A foot surveillance might also be used to

get close to a vehicle entrance or exit to clandestinely photograph the target, his/her vehicle and their protective personnel (if any).

**Technical/Signal(Radio) Surveillance**

The final surveillance method that ***C/T's*** utilize for gathering information on potential targets is Technical/Signal (Radio) surveillance. The most typical tactics used in this type of surveillance is the monitoring of portable hand-held or vehicle radio traffic used by the target and his/her security personnel. This is accomplished by surreptitiously obtaining the radio frequencies used by the target or monitoring open and non-secured (or non-encrypted) radio communication using a radio scanner (commercially available). The ability to listen to a target and his/her security when traveling in a vehicle, and at arrivals and departures provides very timely and important intelligence for attack planning.

## Information Objectives of the Criminal or Terrorist Surveillance

At the end of a comprehensive surveillance operation the ***C/T's*** hopes to have as much information on the following concerning potential targets:

- ☑ The work location of the target.
- ☑ The typical time of arrival at their work location.
- ☑ The typical time of departure from their work location.
- ☑ The residence location of the target.
- ☑ A description of the vehicles used by the target, with license tag numbers.
- ☑ The target's typical time of departure *for* work each day.
- ☑ The target's typical time of *arrival* home from work each day.
- ☑ The most frequent routes from the residence to the work location (and from work to the residence) used by the target (including points of vulnerability, such as choke points).

- ☑ The typical work hours and after-working hours activities of the target [e.g., gym, school, church].
- ☑ The typical routes used by the target to go from his/her work location to regularly scheduled or frequent after-hours activities [e.g., gym, child's school].

- ☑ The normal weekend activities of the target.
- ☑ The visible security around the target while traveling in their vehicle, at their work location and at their residence.
- ☑ An idea of the target's overall attention to their personal security and level of security precautions followed.

After the above information has been collected by the ***C/T's*** they will decide if it is feasible to successfully carry out an attack on the target. If they believe it is feasible, and that it is the best target, they would begin the second surveillance stage of the attack cycle – the pre-attack surveillance.

## Surveillance Detection Techniques

A security aware Executive and professional protection specialists will be aware of the surveillance tactics used by ***C/T's*** in the planning stages of an attack. They consistently practice good surveillance detection. At a minimum, the Executive and protection specialists should have pen and paper on their person when working so that they may record, in a timely manner, the description[s] of either suspicious persons or vehicles observed.

The Executive's vehicle and any security vehicles should also be equipped with a digital camera, and at least one pair of binoculars. The camera would be used to photograph suspicious persons or vehicles observed while the team is moving with the executive, or at locations they are visiting.

Once they have returned to the residence or work location, the photographs should be downloaded onto an office computer for later referral. The Executive, his/her driver, and all executive protection personnel should review the photographs, on a regular basis, so that if a similar suspicious vehicle or person is observed at future locations, appropriate notifications and precautions can be taken. Written notes of suspicious persons, vehicles, and incidents should also be entered into the office computer for later analysis, comparison and follow-up. All written notes, in addition to a description of the suspicious person, vehicle or incident should include details on the "Who, What, Why, When, Where and How" of the incidents.

As mentioned earlier, a security aware Executive and professional protection specialists will always be alert to possible surveillance activity (as described earlier in this article) but will be **especially attentive** for possible ***C/T*** surveillance at the following locations:

- ☑ Within several blocks of the Executive's regular work location and especially near the regular arrival and departure points for his/her security vehicle.
- ☑ Within several blocks of the Executive's residence and especially near the regular arrival and departure points for the executive.

- ☑ Within several blocks of locations that the Executive visits on a regular basis [e.g., gym, church, medical facility].
- ☑ At all choke points and other points of vulnerability along the vehicle routes normally used by the Executive.
- ☑ At the pedestrian entrances to locations regularly visited by the Executive such as their office building, gym, church, etc.

## Surveillance Avoidance Techniques

A security aware Executive and professional protection specialists will attempt to prevent and avoid a successful ***C/T*** surveillance operation by using as many surveillance avoidance techniques as feasible: Some of these techniques are as follows:

- ☑ By departing from the residence for the work location at *different times* each day and by departing from the work location for the residence at *different* times each day [This should be done as many times each week as possible and will, obviously, require the assistance of the Executive and the person who prepares their schedule]. One method for building randomness in the above schedule is to pick five morning departure times and five evening departure times. These should be separated by 15 minutes each. Each of the five departure times should be given a number from one to five. A die can then be rolled to determine which departure time in the morning should be used and which departure time in the evening could be used.

- ☑ By *randomly* selecting the entrances and exits used at the work location when feasible.
- ☑ By using a *wide variety of routes* to and from the residence and work location, and other sites visited on a regular basis, whenever feasible. Randomness can be built into the selection of routes by identifying different routes, numbering each route and then using a roll of a die to determine the routes for the day.
- ☑ By *periodically changing vehicles* used to transport the Executive, whenever feasible. If this tactic is used the vehicles should be of different colors, makes and models. The practicality of this tactic would also have to be evaluated if the Executive uses an armored vehicle, as most Executive's will not have access to multiple armored vehicles.

- ☑ By using a *low-key* and *unobtrusive* a protection profile, whenever possible. The goal would be to attract as little attention to the Executive and their protective measures as possible. This tactic can also include the use of discreet, alternate exits and entrances to a location, so that it would be difficult to pick the Executive out of normal pedestrian or vehicle traffic.
- ☑ By using *deception*. This tactic would involve the use of the Executive's regular security vehicle, that would depart or arrive at a location, BUT without the Executive. A vehicle different from that normally used would then transport the Executive and would use a different arrival or departure location than the deception vehicle (the normal vehicle used by the Executive in this case).
- ☑ By building as much *randomness* into the Executive's daily routine as feasible. This would obviously require the cooperation of the Executive, his/her family, and the person who schedules their daily activities.

## The Importance of Effective Operational Security in Surveillance and Attack Avoidance

Another very important component in any effective surveillance and attack avoidance effort is operational security [OPSEC]. An Executive's and his/her protective team's efforts make a **C/T's** surveillance efforts more difficult but can be defeated by poor operational security. OPSEC, in the executive protection context, is the identification of the C/T's surveillance information objectives, discussed earlier and below, and taking security measures to reduce, conceal or eliminate them. *In cannot be stressed enough that good OPSEC is a crucial requirement for an effective security program for Executives working in high threat environments*.


Some key elements of information that might be made public that could provide valuable information to ***C/T's*** about an Executive's security are:

- ☑ Photos of the Executive.
- ☑ Photos of the Executive's security vehicle.
- ☑ The Executive's schedule.
- ☑ The name of the hotel where the Executive resides when travelling.

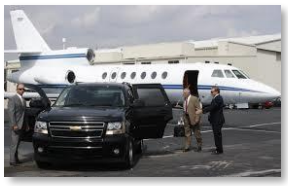

- ☑ The Executive's name when making hotel reservations.
- ☑ The Executive's identity, or making it known, when leasing an Executive's vehicle or protective team security vehicles.
- ☑ Public descriptions of the of the personal security precautions used by the Executive.
- ☑ Publication of the address of the Executive's residence and discussion of the security precautions at the home.
- ☑ Publication of details concerning the Executive's immediate family [including names, ages and photographs of their spouse and children, and the names and locations of the children's schools].

To reduce or conceal the above elements of information from the view of ***C/T's***, the Executive, his/her staff, and any protective personnel will need to work together to have good operational security. OPSEC is also affected by the personal profile of the Executive. High profile Executives or Personalities seek publicity which can, obviously, impact OPSEC. Some basic methods that can be used to improve an OPSEC program are as follows:

- ☑ Limit the public distribution and use of photos of the Executive, their security vehicle, and family to an approved list of trusted employees. In many cases, the Executive will have an official organization photo that is published, or have their photo taken in public that is later published and this precaution cannot be used. For those who maintain a lower profile this precaution should be used as much as feasible.

- ☑ Limit the public and internal distribution of the Executive's schedule to as small a group of trusted individuals and employees as possible. Maintaining a close hold on the Executive's schedule of activities is one of the most important precautions that can be implemented.
- ☑ Limit the publication of the address of the Executive's residence to the smallest group of trusted individuals as possible. This precaution also extends to the publication of their address in any of their organization/s employee telephone/address directories, etc.
- ☑ Minimize the awareness of the Executive's restricted parking space in the garage by not using the most obvious space and using non-specific parking space signage.

- ☑ Minimize the obvious signals an Executive emits when departing from a location. This tactic can be implemented by ensuring that the Executive's vehicle and/or any security vehicles, do not arrive too early at the expected departure point, signaling the Executive's imminent departure. It would also include minimizing significant, *highly visible* security activity before their arrival and departure from a location.
- ☑ Minimize any discussion of the Executive's security to the minimum number of trusted individuals possible. Media requests for such details should always be refused.
- ☑ Minimize, whenever feasible, public discussion of details of the Executive's family, including publication of their photos.
- ☑ Minimize, whenever possible, the use of the Executive's name when registering at a hotel. The name of the hotel to be used by the Executive should also be restricted to the minimum number of individuals necessary. The room should also be rented in the name of a staff member, whenever possible. It is also suggested that a non-corporate credit card be used and the identity of the organization renting the rooms be minimized when circumstances permit.



- ☑ When utilizing an organization's, or leased plane for travel, the name of the organization or Executive should not be painted and visible on the exterior of the plane.

## Conclusion

This report was a ***concise*** attempt to discuss the key role target surveillance plays in the ***C/T*** planning cycle, especially for kidnapping and assassination attacks. The report explained how ***C/T's*** use surveillance in selecting targets and in the planning and execution of attacks. It discussed the types of target information ***C/T's*** collect, how to detect and avoid surveillance, and the importance of OPSEC in an executive protection program. Hopefully, the report will assist Executives and protection specialists to better protect themselves in high threat locations.

# EXECUTIVE SECURITY CHECKLIST

## 1. GENERAL PRECAUTIONS

- ☐ Are you keeping your profile as "low" as possible?
- ☐ Are family members, residing overseas with you, keeping their profiles as low as possible?
- ☐ Has your office and residence staff been instructed **not** to give out personal details about you to others without first, obtaining your permission?
- ☐ Are you randomly selecting your departure times and travel routes from *home* to *work* on a regular basis?
- ☐ Are you randomly selecting your departure times and routes from *work* to *home* on a regular basis?
- ☐ Are you randomly selecting your departure and arrival times, and travel routes, to and from places, other than work, that you visit on a regular basis (e.g. children's school, gym, church)?
- ☐ Are you, your family, residential staff, driver and any security escorts checking for suspicious persons and vehicles whenever they are approaching or departing your work site, residence or places you visit on a regular basis? Are they aware of what action to take if they observe possible surveillance?
- ☐ Have you been maintaining good situational awareness sand practicing effective OPSEC to prevent and avoid security related incidents?

## 2. EXECUTIVE PROTECTION

- ☐ Have you had a comprehensive threat and risk analysis completed on yourself by a qualified security professional?
- ☐ Do you have a professionally developed Executive Protection Plan that includes detailed written policies and procedures for yourself, your staff, your family, your office driver (if any) and your executive protection team (if you have one)? The plan should also include a comprehensive security plan for your office, residence, and when traveling.
- ☐ At a minimum, has your driver been trained in basic security driving responsibilities and techniques? (The responsibilities should be detailed in your Executive Protection Plan)
- ☐ If you have an Executive Protective Team, were they thoroughly vetted before their employment, and periodically thereafter? This should include, at a minimum, criminal history checks, personal security interview, reference checks, physical fitness test, and medical screening (including drug testing).
- ☐ If you have an Executive Protective Team, have they received training in executive protection techniques from a reputable training entity? Do they receive annual refresher training?
- ☐ Does your Executive Protective Team have the necessary equipment and organization support to provide effective service?