



# Homeland Security



**STUDENT REFERENCE**  
Surveillance Detection Training for  
Commercial Infrastructure Operators and Security Staff



# Homeland Security

## STUDENT REFERENCE

**Surveillance Detection Training for  
Commercial Infrastructure Operators and Security Staff**

*Aug/Sept 2006*

**ARMORGROUP**  
INTERNATIONAL TRAINING, INC.



## TABLE OF CONTENTS

### **Preface**

### **Module 1**

Course Overview/Objectives/Handouts/Logistics

Pre-course Assessment

### **Module 2**

Lesson 1 (part 1)

Attack Methodology/Attack Cycle/Pre-incident Indicators

Lesson 1 (part 2)

Vulnerability Analysis

Lesson 2

Vulnerability Analysis Practical Exercise

### **Module 3**

Lesson 1

Area Analysis/Hostile Surveillance Positions (Red Zone)

Lesson 2

Red Zone Design Practical Exercise

Red Zone Exercise Debrief

Lesson 3

Surveillance Detection (SD)

Lesson 4

Surveillance Detection Position Practical Exercise

SD Exercise Debrief

### **Module 4**

Lesson 1

Developing the Surveillance Detection Plan

Lesson 2

Observation and Reporting

### **Module 5**

Critical Infrastructure Buffer Zone Capstone Exercise

Exercise Debrief with Role Players (if used)

Post-course Assessment

### **Course Conclusion**

Review Post-course Assessment

Course Critique

Graduation (present certificates)

### **Glossary**

**Addendum – DHS Suspicious Incident Categories**

**References**

## PREFACE

Facility security encompasses three basic rings: the physical ring, which includes security measures such as locks, fences, bars, and barriers; the procedural ring, which includes things such as badges and access procedures; and the invisible ring, or information ring of security.

Through classroom lectures and hands-on exercises, instructors emphasize the importance of recognizing that visible security measures (physical and procedural rings of security) can ultimately be defeated by the attacker. While industry should continue to use physical and procedural security measures, the goal is for students to understand and employ the three Defensive Measures encompassed by the invisible ring of security. Training focuses on teaching potential targets how to integrate and use the information ring, greatly increasing their overall level of security awareness.

Instructors explain how terrorist attacks, regardless of where they occur, are planned and executed. Case study analyses confirm that when targets are surprised by an attack, the target's time to react is seconds (some estimate less than 5 seconds), and the result is usually the loss of life. The body's response to surprise makes it difficult or even impossible for the target to respond effectively. In the time it takes a target to plan a response, the attack is over and the damage is done. Understanding the attack cycle and employing the three Defensive Measures can greatly increase a potential target's chances of avoiding an attack altogether, or effectively responding to it, thereby increasing the odds of survival.

Based on testimonials of individuals who have been attacked and employed these strategies, the system works. The key is to practice the systems approach to facility security. ***Your training will focus on the Surveillance Detection defensive measure.***



# Homeland Security

## Student Reference

### Surveillance Detection Training for Commercial Infrastructure Operators and Security Staff

#### **Scope of Training and Course Goal:**

Provide students with the knowledge to develop a Surveillance Detection Plan.

#### **Course Learning Objectives:**

1. Employ fundamentals of Surveillance Detection related to a facility (or system).
2. Develop actionable Surveillance Detection plan.
3. Report observations with necessary details to aid security officials in their efforts.



## **Module 1:**

### **Course Introduction**

Instructor(s)  
Company Background  
Student Introductions  
Safety Concerns  
Course Design and Student Tasks  
Pre-course assessment

#### **Terminal Objective:**

- Determine students' baseline knowledge

#### **Enabling Objectives:**

Students will:

- Recall the basic course outline, student tasks and attendees.
- Complete a pre-course assessment related to course concepts.

## **Module 2 Lesson 1, Parts 1 & 2:**

Terrorist Attack techniques/methods  
Five Defensive Measures  
Attack Cycle  
Rings of Security  
Pre-incident Indicators  
Components of Vulnerability Analysis

#### **Module 2 Terminal Objective:**

Following Lesson 1, parts 1 and 2 and given the exercise worksheet found on page 8 of this guide, students will conduct a Vulnerability Analysis (FVA) and brief the instructors on their findings.

## Lesson 1 (part 1):

### Module 2:

#### Lesson 1 / Part 1 Enabling Objectives:

When students complete this module, they should be able to:

- Recall terrorist attack trends, techniques/methods
- Recall security measures and outcomes
- Recall the three rings of security and explain the importance of each.
- Recall the 7-step attack cycle
- Describe the detectable points (weak links) within the attack cycle

## Terrorist Attacks

Current trends:

- Against facilities –

IED (improvised explosive device)

VBIED (vehicle born improvised explosive device)

- Against personnel -

IED  
VBIED  
Small Arms

Why are these attack models used?

1. Because they work!
2. Have low or easily met equipment needs.
3. Are easily trained & exported.

Fortunately, to date, there have been few attacks on US soil.

However, we must note that attack trends worldwide provide us with information about what the trends will be in the U.S.

**NOTES:**

## How do we protect ourselves against the threat?

### Security Measures & Outcomes:

#### Measures:

Identify  
Implement  
Detect

#### Outcomes:

Avoid  
Deter  
Counter

### Rings of Security:

#### Physical (visible) -

Walls  
Fences  
Gates  
Guards  
Plantings

#### Procedural (visible) –

ID checks  
Entry badges  
Access coded entry  
Alarms systems  
CCT  
Cameras

#### Information ring –

Information about the threat that comes from the outside.

Information that the opposition does not know you have

NOT VISIBLE – more difficult to defeat

### Facility Security

#### Three Rings of Security

Physical  
Technical /  
Procedural  
Information /  
Intelligence



3/21/06

11

### Attack Basics:

#### Attackers look for soft targets -

- Soft targets are predictable.
- Soft targets often rely only on physical and procedural security measures.
- The focus of most facility security is from the inside looking out.
- Facility personnel not trained on targeted awareness (where to look and what to look for)
- When security has to engage in the interdiction (reaction) phase, it might already be too late

What if you looked at security from the viewpoint of the attacker?



## **The Attack Cycle / Pre-incident Indicators (steps 2 and 4 in the attack cycle)**

Because facilities are stationary, establishing predictability related to activity surrounding the building is required, Surveillance Detection is the specific activity that is the key to recognizing and deterring an attack. If surveillance is not detected, then you are left with the tool of Attack Recognition to interrupt the terrorist attack cycle at the last moment in order to thwart an attack. Since the latter only gives you a few seconds, or maybe minutes, to react, Surveillance Detection is the process of choice in order to thwart the terrorist attack cycle. Therefore, developing and employing an effective Surveillance Detection Plan is the key to maximizing security posture.

### **ATTACK CYCLE**

- 1. Target List**
- 2. Surveillance**
- 3. Final Selection**
- 4. Planning/Surveillance**
- 5. Attack Team Deployed**
- 6. Zero Hour**
- 7. Action:**
  - attack**
  - IED**
  - Kidnapping/hostage**
  - etc...**

Attackers are most vulnerable in steps two and four.

**Steps 2 and 4 offer opportunities to detect surveillance and take action to deter an attack.**

Once zero hour has been determined and the attack has been initiated, Attack Recognition and Response is the best hope for ensuring the safety of individuals in and near the facility.

**Breakout Group Activity:**  
How do terrorists pick their targets?

**What information is needed?**

**What information is considered  
general information?**

**What information is considered  
mission critical?**

**What methods can terrorists use to  
gain this information?**

**Module 2:**

**Lesson 1 / Part 2 Enabling Objectives:**

When students complete this module of instruction they should be able to:

- Recall the 8 components of a vulnerability analysis
- Recall predictable activities associated with a facility

**Facility Vulnerability Analysis:**

- Facility Vulnerability Analysis (FVA) is the method used to determine facility vulnerability as well as predictable activity surrounding the facility.
- It is necessary to view the facility and its weaknesses **from the perspective of the attacker** (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 us to see the situation as the attackers would/will, and could ultimately enable us to thwart their plans.

**Surveillance Methodology and the Analysis Mind Set:**

**Surveillance** (completed in two phases:

Phase 1: Area Analysis  
(Hostile Surveillance Requirements)

Phase 2: Facility Analysis  
Site-Specific Vulnerabilities  
Determines Location of Attack  
Determines Type of Attack

**Phase 1 of 2**

**8 Facility Vulnerability Components:**

1. \_\_\_\_\_
2. \_\_\_\_\_
3. \_\_\_\_\_
4. \_\_\_\_\_
5. \_\_\_\_\_
6. \_\_\_\_\_
7. \_\_\_\_\_
8. \_\_\_\_\_

**Predictable activities associated with a facility include but are not limited to:**

- Service calls/scheduled deliveries
- Regularly scheduled visitors/events
- Standard workday comings and goings of personnel
- Procedure/drill practices
- Regular services provided to the public, such as visa or permit lines.

**What predictable activities associated with your facility can be exploited by an attacker?**

## Module 2/Lesson 2

### Vulnerability Analysis Practical Exercise #1:

**Objective:** With the guidance of the instructor and the handout provided, your task is to conduct a vulnerability analysis identifying the critical vulnerabilities of a specified facility and brief your classmates and the instructor on your findings.

#### Definitions

**Area denial** – areas where personnel and possibly vehicles are denied access.

**Area minimization** – areas where access is restricted based upon specific requirements for entry.

**Portal** – an entry way into the facility either for personnel or vehicles.

**Uncontrolled areas** – those areas that are not controlled by the company/owner or its security personnel in regards to occupation or travel through the area by others.

#### Performance Objective

**Task** - Conduct a facility vulnerability analysis.

**Condition(s)** – given a designated facility, the student work sheet supplied by the instructor and your student guide, take an “outside looking in” approach to the vulnerability analysis.

**Standard** – complete a vulnerability analysis addressing the eight key areas of the facility and identify the primary facility vulnerability.

#### #1 General Building Design



#### #2 Proximity to uncontrolled areas



**Vulnerability Analysis Worksheet, cont.**

**#3 Portals**

A large, empty rectangular box with a black border, intended for handwritten notes or analysis related to the '#3 Portals' section.

**#4 Barriers**

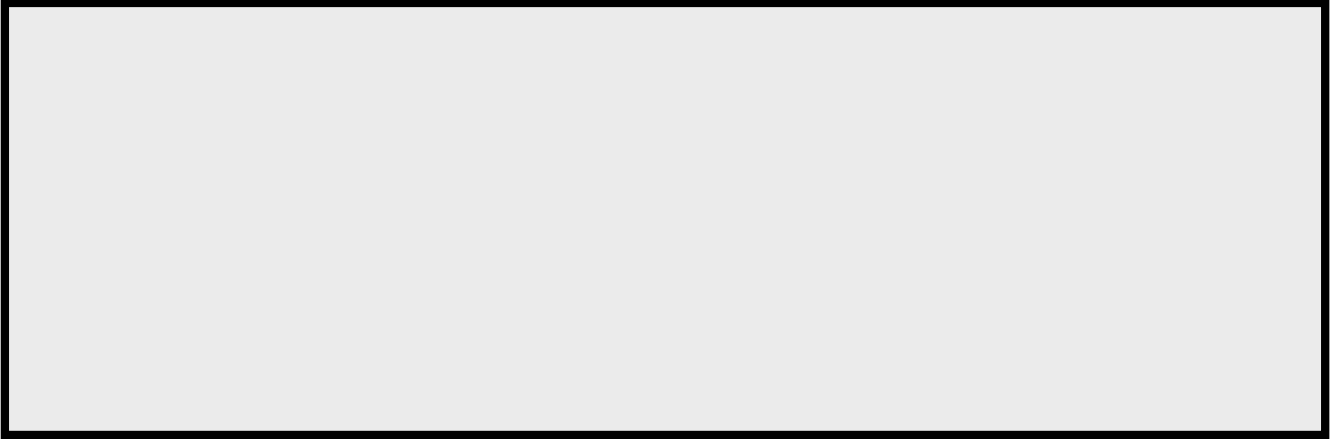
A large, empty rectangular box with a black border, intended for handwritten notes or analysis related to the '#4 Barriers' section.

**#5 Access by uncleared personnel**

A large, empty rectangular box with a black border, intended for handwritten notes or analysis related to the '#5 Access by uncleared personnel' section.

**Vulnerability Analysis Worksheet, cont.**

**#6 Access by required services**

A large, empty rectangular box with a black border, intended for handwritten notes or diagrams related to item #6.

**#7 Area denial to access**

A large, empty rectangular box with a black border, intended for handwritten notes or diagrams related to item #7.

**#8 Areas minimized to access**

A large, empty rectangular box with a black border, intended for handwritten notes or diagrams related to item #8.

## Module 3: Area Analysis

### Lesson 1 – Area Analysis for the purpose of determining the Red Zone and Hostile Surveillance Positions (HSP)

#### Module 3 Terminal Objective:

Identify Surveillance Detection Positions

#### Enabling Objectives:

Upon completion of this module, students should be able to:

- Lesson 1- Recall the basic requirements of Red Zone design.
- Lesson 2- Design a Red Zone and identify HSPs related to a specific location.
- Lesson 3- Recall the basic requirements of Surveillance Detection (SD) positions.
- Lesson 4- Select SD positions in support of a specific location.

#### Purpose of Area Analysis

Area analysis is the process by which we identify the general areas and specific locations attackers can/will use to perform surveillance on the facility's vulnerabilities, avenues of approach, and nearby activities that may aid in planning/carrying out the attack. These identified areas are known as the **Red Zone(s)**.

**The Red Zone** offers an attacker:

Surveillance Requirements-

- View of the target facility, **specifically the target's vulnerabilities**
- Cover and/or concealment (ability to be unnoticed or hidden)
- Entry and exit routes (ability to enter the area safely and leave with the collected information)

#### Consider the following:

- Surveillance Detection must visually cover the Red Zone in order to detect surveillance.
- SD does not have to see the target in order to detect
- Analysis tells SD where the attackers have to go to gather the information they need
- Having "eyes on" the target and its vulnerabilities may help to establish correlation between a target and a surveillant

#### Consider the following:

- Does the Red Zone of a particular facility change when the seasons change?
- Is the Red Zone of a particular facility different in daylight and nighttime?
- Does the Red Zone change during special events?
- Due to limited resources, the smallest, most clearly defined physical, geographic space is optimal when analyzing the Red Zone.



**Module 3/Lesson 2 Practical Exercise:**

**Area Analysis Red Zone and Hostile Surveillance Positions**

**Practical Exercises #2 & #3** (the same worksheets are used for both practical exercises)

**Definitions**

**Concealment**

To be concealed is to be hidden from view.

**Cover**

Blending into the surroundings or having a reason to be in a specific location.

**Covert**

Surreptitious or done with a purpose for other than what is apparent.

**Profile vs. Signature**

What someone looks like verses what they are doing.

**Red Zone**

Areas hostile surveillance can occupy to observe an intended target's vulnerabilities.

**Surveillance Detection**

The process of determining whether or not surveillance is present.

**Surveillance Site**

A location where the attacker can see the target, has a reason to be there (cover) or be hidden from view (concealment), and has a reasonable, plausible entry and exit.

**Performance Objective**

**Task** - Conduct an Area Analysis.

**Condition(s)** – given a designated facility, the student work sheet supplied by the instructor and your student guide, take an outside looking in approach to the area analysis.

**Standard** – complete an area analysis to include identifying potential hostile surveillance locations, their view of the vulnerability, potential cover/concealment possibilities, possible entry/exit and provide a sketch of the “Red Zone” related to the designated facility.

Finally, as part of a follow on exercise - identify potential Surveillance Detection positions (locations, view of the Red Zone, potential cover/concealment, entry/exit relative to the “Red Zone”).

**Identify potential hostile surveillance positions**

Location(s) with a view of the target's vulnerability

**Area Analysis Practical Exercise, cont.**

Cover and/or concealment potential

Entry and exit potential

Within the space provided, sketch the "Red Zone"

**Area Analysis Practical Exercise, cont.**

**Surveillance Detection locations**

Locations(s) with a view of the Red Zone

Cover and/or concealment potential

Entry/exit potential

## Module 3/Lesson 3: Surveillance Detection

Case studies reveal that surveillance is the weakest link in the attack cycle. Often, initial surveillance (step 2) is poorly executed due to lack of discipline or training of the surveillance team. Additionally, surveillance generally occurs over a period of time (the earlier in the cycle, the longer), providing potential targets with opportunities to observe correlations and identify mistakes made by hostile surveillance.

Surveillance Detection is the on-going process by which we focus various assets on the identified Red Zone areas to detect surveillance in those areas. We use the Surveillance Detection Pyramid to illustrate the components of the process.

### Purpose of Surveillance Detection

To determine whether or not surveillance is being conducted on a specific facility.

### Location

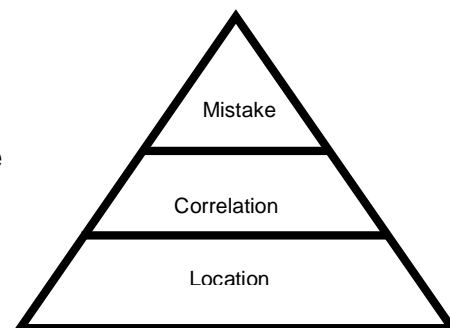
The areas of the facility identified during area analysis as being likely surveillance locations (Red Zone) allowing observation of the target and specifically the vulnerability of the facility.

### Correlation

Correlation is any activity directly corresponding to the facility or target. Individuals engaged in Surveillance Detection should look for and note any:

- Repeated sightings over time related to vulnerable areas or predictable facility activities.
- Repeated sightings related to facility service calls or delivery areas.
- Same person surveilling different facilities.
- Different people surveilling same facility.

### SD Pyramid



### Mistakes

Surveillance team members often make mistakes. Their mistakes provide individuals engaged in Surveillance Detection with opportunities to discover their presence. Look for and note:

- Individuals whose profile and signature do not match.
- Individuals signaling others when specific activities occur at the facility.
- Individuals checking the time, making a call, photographing the facility, or taking notes.

## Handling the Red Zone:

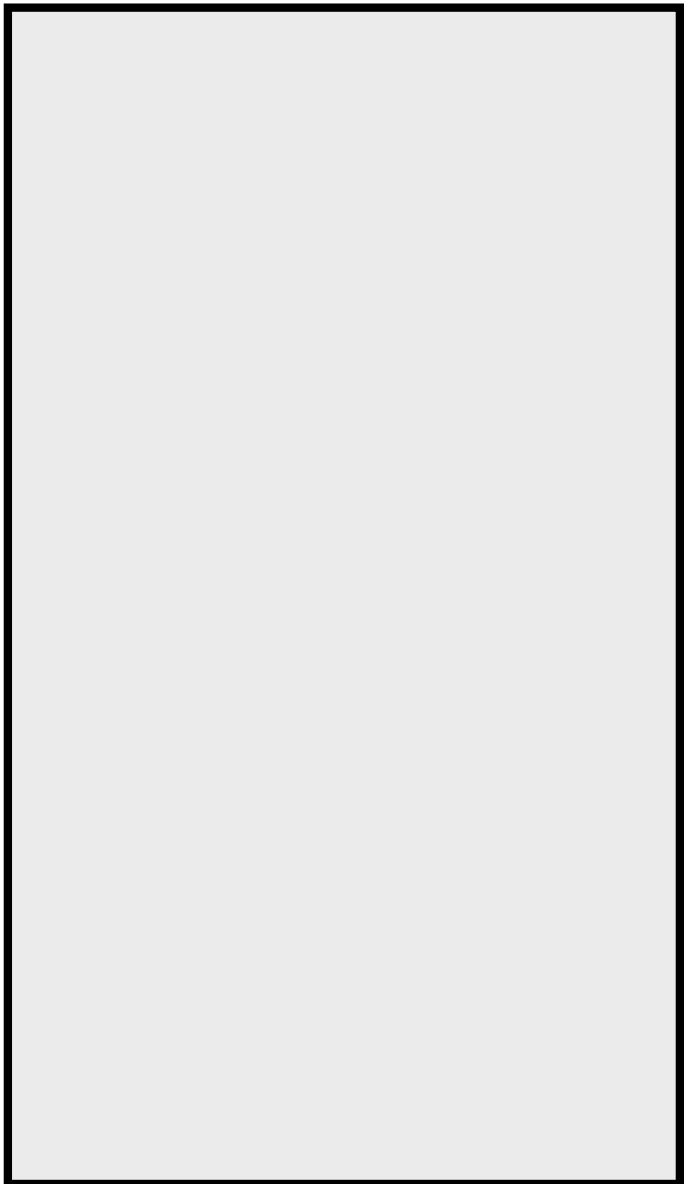
Identifying the Red Zone is also a safety precaution for Surveillance Detection assets.

A Surveillance Detection presence *inside* the Red Zone should be avoided unless **perfect cover** can be established for SD.

Without perfect cover, it is too easy for the attackers to discover the SD assets and “plan their way around them” by relocating, modifying their collection efforts or “dealing with” the Surveillance Detection team members directly.

SD is safest from outside the Red Zone, either from within the protected facility itself, or from positions outside the Red Zone looking in at the back of the surveillance members as they are watching the facility vulnerabilities.

It is not necessary for SD to see the actual vulnerabilities or the facility itself (they will not change/relocate unexpectedly), but rather focus their attention on the Red Zone, looking for surveillance activity.



## Surveillance Detection and Profile vs. Signature

### **PROFILE**

**What someone looks like**

**Vs.**

### **SIGNATURE**

**What someone is actually doing**

Even when in condition yellow, potential targets can be fooled by the activities and appearances of others.

Profile vs. signature refers to what a person looks like vs. what they are actually doing.

When looking for possible surveillance activity, ask yourself if the person you are observing seems to be doing what their appearance tells you they should be doing.

Some examples are of profile vs. signature as follows:

A truck marked with a delivery logo should be making frequent stops, not parked for long periods of time.

Tourists travel in pairs or groups and take pictures of tourist attractions, not individual homes or government facilities.

Cars break down in inconvenient locations and drivers appear frustrated as they try to correct the problem or summons help.

Construction workers wear hard hats and work boots. They are focused on the task and not standing idle watching traffic, jotting notes or signaling.

**What profile could hostile surveillance be using for cover in the Red Zone of your facility?**

#### **Lesson 4:**

##### **Selecting Surveillance Detection Positions Practical Exercise**

The instructor will provide guidance related to a designated facility for use during the exercise. A student work sheet will also be provided. Your task is to select potential surveillance detection positions using all previous course work (vulnerability analysis, Red Zone Design) and brief your classmates and the instructor on your findings.

#### **Module 4:**

##### **Facility Surveillance Detection Planning and Observation Skills**

###### **Terminal Objective:**

Using the information gathered, develop a Surveillance Detection Plan.

###### **Enabling Objectives:**

When students complete this module, they should be able to:

- Lesson 1- Recall the key elements of facility SD planning.
- Lesson 1- Recall the key questions for facility SD planning.
- Lesson 2- Demonstrate the ability to observe and recall details of appearance and behavior.

## Module 4

### Lesson 1: Developing the Facility Surveillance Detection Plan

Planning is often the most neglected component of facility security. This condition exists due to multiple factors that can confuse even the most adept planner. The (5) elements of the Facility SD plan, coupled with the (5) questions for a SD plan can provide security planners of all levels with a quick, and easy to use reference for ensuring a thorough Surveillance Detection plan for their facility.

The security planning process is one that should be constantly refined because it is a process driven by the surrounding environment and the activities within that environment. The five elements of Facility SD allow for a strong planning foundation that requires only minimal adjustment over time due to environmental changes.

The five questions for Facility SD, once answered, should serve as the basis of the SD portion of a facility's security SOP (Standard Operating Procedure). These questions also help the planner find the inherent weakness of the security plan so that risk mitigation can take place. In order to do this the following equation is used:

#### The five elements of the SD Plan:

1. Vulnerability Analysis
2. Area Analysis (AA)
3. SD Team Positions
4. Reporting
5. Interdiction

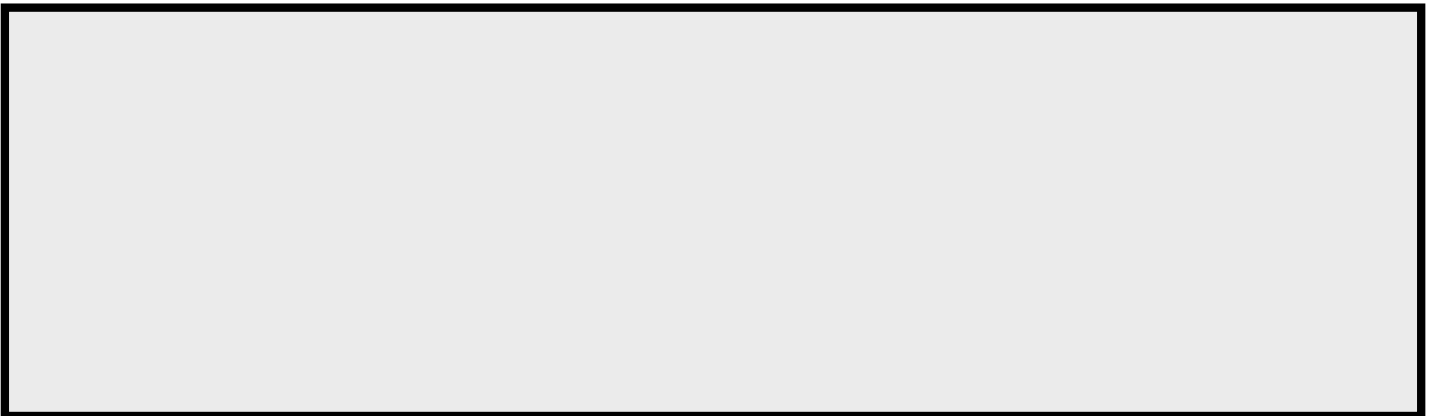
---

#### The 5 Questions for the Facility SD Plan:

1. What are your capabilities and limitations (resources)?
2. Where are you looking to and from?
3. What are you looking for?
4. Where does the information go?
5. Who acts on the information?

### SECURITY PLANNING EQUATION: Ideal Plan – Realistic Plan = Planning Weakness

The first elements of the plan have shown us where to look and what to look for. Now we can turn our attention to reporting the information we obtain to those who can do something with the information.



## Reporting

**Remember, the information we provide must enable the receiver to act!**

Ensure timely reporting by organizing your information so that security or law enforcement officials can use it to take action. Report using the following format:

- WHO is doing WHAT?
- WHEN did they do it?
- WHERE did they do it from?
- HOW did they do it?
- WHY they were doing what they did (if you can determine this)?

Cover these items with quick, complete, accurate information and you will have accomplished a great deal when it comes to your part – Surveillance Detection.

Also, remember the methods available to you:

person to person	email
telephonic/mobile phone	fax

Keep your role firmly in mind. As a private citizen you are not in a position to perform a function beyond observing and reporting the activity that has drawn your attention.

Interdiction of that activity should be left to officials who have the sworn authority to act upon your information.



## Module 4/Lesson 2: Observation Skills

**“Observation is more than seeing; it is knowing what you see and comprehending its significance.”**

- Charles Gow

### **Terminal Objective:**

Accurately identify individuals and vehicles using “identifying “ characteristics.

### **Enabling Objectives:**

When students complete this module, they will be able to:

- Identify distinguishing physical characteristics
- Identify changing physical features
- Identify changing details of appearance or behavior
- Recall factors that affect observation skills and recall
- Practice methods for improving observation skills and memory

Observation is the ability to take specific notice, recognize, remember and accurately describe someone’s physical characteristics and behavior. Observation skills apply to vehicles as well.

It is a skill set which involves all the senses and the memory, which can be improved with purposeful practice.

Good descriptions go from the general characteristics of a person to very **specific identifying characteristics** such as:

### **General Characteristics:**



Sex  
Race  
Height  
Weight  
Age

### **Identifying Characteristics:**

facial features -  
    cheek bone structure, dimples  
    shape of nose, chin,  
    ears  
    mouth (shape of lips, teeth)  
eyes (color, shape, distance between)  
complexion  
mannerisms  
shape of the head  
abnormalities  
scars  
voice  
characteristic physical movement

Remember, general descriptions alone will not provide enough detail to assist law enforcement and security officials in their efforts to find and perform their duties concerning the situation.

Include general, but be sure to focus on *identifying characteristics*. Your description has to allow someone to pick a person out of a crowd, literally.

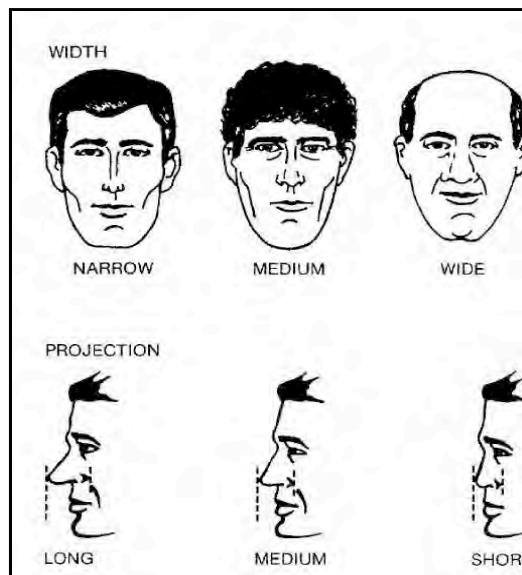
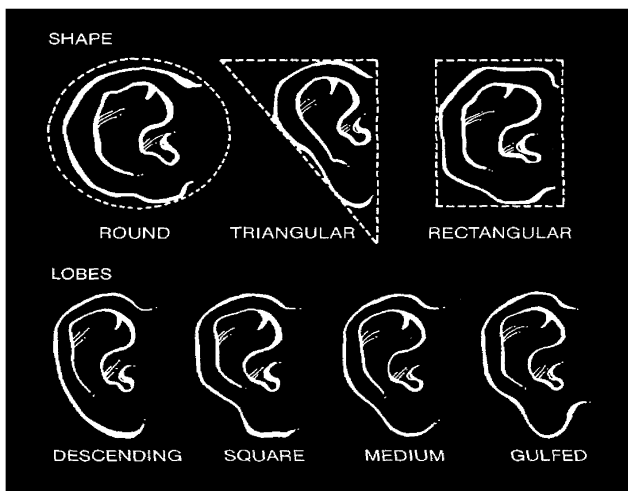
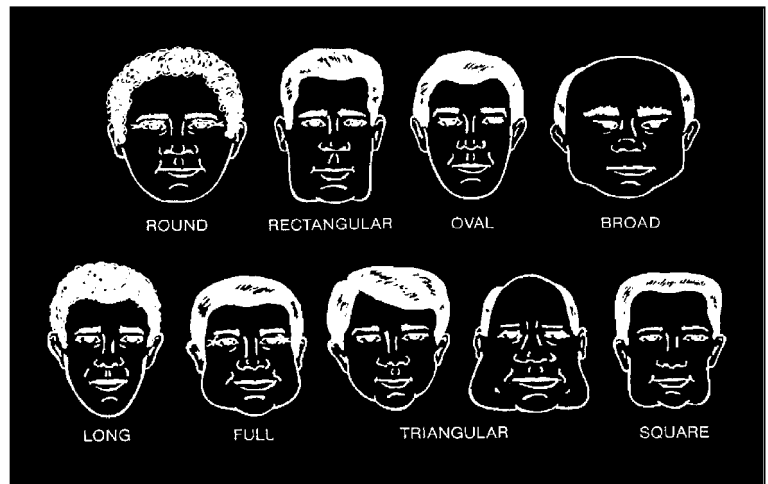
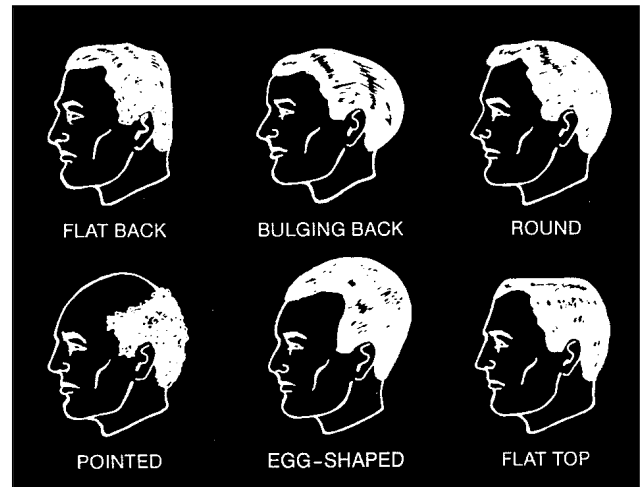
If your characteristic is a number, use a range rather than a specific.

Practice your observation skills to improve your ability to accurately recall specific information.

**Bertillon's Identifying characteristics:**

Bertillon's anthropometrical system of personal identification is divided into three integrated parts:

1. The bodily measurements.
2. The appearance and shape of the body.
3. A description of any peculiar marks which could have resulted from but are not limited to:
  - Disease
  - Accident
  - Deformity
  - Disfigurement
  - Moles
  - Warts
  - Scars
  - Tattoos, etc...



## Changeable Features

- Clothing and footwear
  - Type, color and style of clothing
  - Headgear, shoes
- Jewelry
  - Watch, necklace, earrings, eyeglasses, rings...
- Hair and hair style
- Accessories and Props
  - Cameras, backpacks, bags, cell phones...

## General Characteristic Vehicle Examples



- Type
- Color
- Size
- Make
- Model
- Number of doors
- License
- Year

...and note distinguishing features

## Factors that Affect Observation Skills

- Time
- Physiological
- Psychological
- Location and Position
- Weather and Light Conditions
- Behavioral and Cultural Attitudes

## Methods to Improve Observation Skills

- Be alert and aware
- Use systematic / whole approach
- Find distinguishers
- Keep sense of time
- Improve knowledge
- Practice

*and...*

## Methods to Improve Memory

- Maintain Health and Nutrition
- Organize Yourself

**FOCUS - The art of memory is the art of attention**

**consider also...**

- Visualize - Take a mental picture
- Select and anchor
- Caricaturize - Pin a moniker
- Rehearse - Elaborate and repeat

**and most importantly...**

**Review:**

When attempting to describe a person who is potentially hostile surveillance, remember to proceed from the general characteristics to the details of their features or distinguishing characteristics. Do not allow those features or details that can be easily changed, such as clothing, hair, jewelry, makeup and props to distract you from the important task of remembering the distinguishing characteristics of the face and body of the person who has caught your attention.

When actively observing you should –

- Remain alert
- Use a systematic approach
- Search for distinguishing characteristics
- Maintain your sense of time
- Improve your knowledge and practice the skill

Your knowledge and memory can be improved by maintaining your health and being organized while observing. Remember that visualizing what you have seen and using a moniker (e.g., Popeye, Robert Redford, Lucy) to describe the person often helps you to maintain the images. Using an anchor point within the characteristics and rehearsing the description will help, but nothing works like writing it down as soon as possible.



## Module 5: Surveillance Detection Capstone Exercise

### **Terminal Objective:**

Detect surveillance using the methods and techniques learned throughout the course.

### **Primary Enabling Objectives:**

When students complete this module they should be able to:

- Detect and accurately report surveillance activities related to a designated facility.

The instructor will provide guidance related to a designated facility for use during the exercise. A student work sheet will also be provided. Your task is to conduct surveillance detection using all previously completed course work, detect members of a surveillance team targeting the facility, generate accurate physical descriptions, descriptions of any associated vehicles and report these during the out brief to your classmates and the instructor. The Red Team, or surveillance team, will also out brief the students on their activities during the allotted time period.

Standard –

- Given the vulnerability analysis, the Red Zone and the Surveillance Detection positions selected during the course work - occupy the surveillance detection positions and detect the majority of the members of a hostile surveillance team operating against the designated facility.
- Provide accurate descriptions of hostile surveillance team members and their vehicles where this applies.

## Surveillance Detection Capstone Exercise #4

### Definitions

#### **Attack Recognition**

Recognizing the signature of an attack before it actually occurs enabling a trained target to respond appropriately.

#### **Concealment**

To be concealed is to be hidden from view.

#### **Conditions of Awareness**

ArmorGroup International Training uses a color code to teach levels of situational awareness:

- Condition White—oblivious to surroundings or focusing only on task at hand
- Condition Yellow—alerted to surroundings
- Condition Orange—possible threat identified
- Condition Red—engaged with threat
- Black—shock, unable to respond to the situation

#### **Correlation**

Any movement or activity that directly corresponds with our movement or activity.

#### **Cover**

Blending into the surroundings or having a reason to be in a specific location.

#### **Covert**

Surreptitious or done with a purpose for other than what is apparent.

#### **Dry Run**

Practicing an attack on the target in or near the attack site to validate the plan, confirm that the target can be controlled, establish timing, and make the necessary adjustments to successfully complete the attack.

#### **“Log Normal”**

The act of documenting typical activity in APTs .

#### **Profile vs. Signature**

What someone looks like verses what they are doing.

#### **Red Zone**

Areas hostile surveillance can occupy to observe an intended target’s vulnerabilities.

#### **Surveillance Detection**

The process of determining whether or not surveillance is present.

#### **Surveillance Site**

A location where the attacker can see the target, has a reason to be there (cover) or be hidden from view (concealment), and has a reasonable, plausible entry and exit.

### Performance Objective

**Task** – Detect and accurately report surveillance.

**Condition(s)** – given a designated facility, your past vulnerability analysis, area analysis, Red Zone sketch, selected surveillance positions, the student log sheet supplied by the instructor and your student guide, occupy surveillance detection positions outside the Red Zone and detect hostile surveillance.

**Standard** – as part of a team effort, detect or identify the majority of the hostile surveillance team.

**Identify and record potential Hostile Surveillance:**

Location	Time	Description(s) Personnel/Vehicles	Behavior	Remarks

## **GLOSSARY**

### **Attack Recognition**

Recognizing the signature of an attack before it actually occurs enabling a trained target to respond appropriately.

### **Concealment**

To be concealed is to be hidden from view.

### **Correlation**

Any movement or activity that directly corresponds with our movement or activity.

### **Cover**

Blending into the surroundings or having a reason to be in a specific location.

### **Covert**

Surreptitious or done with a purpose for other than what is apparent.

### **Dry Run**

Practicing an attack on the target to validate the plan, confirm security, establish timing and make the necessary adjustments to successfully complete the attack.

### **“Log Normal”**

The act of documenting typical activity.

### **Profile vs. Signature**

What someone looks like compared to what they are doing.

### **Red Zone**

Areas a surveillant can occupy to observe an intended target's vulnerabilities.

### **Surveillance Detection**

The process of determining whether or not surveillance is present.

### **Surveillance Site**

A specific location within the Red Zone where the surveillant can see the target's vulnerability, has a reason to be there (cover) or be hidden from view (concealment) and has a reasonable, plausible entry and exit.



## **Suspicious Incident Categories**

### **ELICITING INFORMATION**

Questioning facility personnel about a facility; this includes individual probing employees in person on or off-site, over the phone, or via the Internet about particular structures, functions, and personnel procedures at the facility.

### **INTRUSION**

Unauthorized personnel entering a restricted area.

### **ATTEMPTED INTRUSION**

Unauthorized personnel attempting to enter a restricted area.

### **PHOTOGRAPHY**

Taking still or moving pictures of a facility.

### **OBSERVATION**

Showing unusual interest in a facility; for example, observing it through binoculars, taking notes, drawing maps, or drawing structures of the facility

### **THEFT**

Stealing something associated with a facility.

### **SABOTAGE/TAMPERING/VANDALISM**

With malicious intent, damaging, manipulating, or defacing part of a facility.

### **CYBER ATTACK**

Compromising, or attempting to compromise, a facility's IT infrastructure.

### **EXPRESSED THREAT**

Making a spoken or written threat to damage or compromise a facility.

### **FLYOVER**

Flying an aircraft over a facility; this includes any type of flying vehicle, including an unmanned aerial vehicle loitering over a site.

### **WEAPONS DISCOVERY**

Discovery of small arms or explosives at or near a facility.

### **OTHER**

Incidents not fitting any of the above categories.

## Excerpt from an al-Qaeda Operations Manual

The brother/photographer should use a modern camera that can photograph at night or from a distance, and only the lens of the camera should be visible...If possible, panoramic pictures should be taken. That is, the collection of views should be continuous in such a way that all pictures are taken from one location and that the ending of one picture is the beginning of the next.

**Information Sources:** Any organization that desires to raise the flag of Islam high and proud must gather as much information as possible about the enemy. Information has two sources:

**Public Source:** Using this public source openly and without resorting to illegal means, it is possible to gather at least 80% of information about the enemy. The percentage varies depending on the government's policy on freedom of the press and publication. It is possible to gather information through newspapers, magazines, books, periodicals, official publications, and enemy broadcasts.

**Secret Sources:** It is possible, through these secret and dangerous methods, to obtain the 20% of information that is considered secret. The most important of these sources are:

- Individuals who are recruited as either volunteers or because of other motives
- Recording and monitoring
- Photography
- Interrogation
- Documents, by burglary or recruitment of personnel
- Drugging
- Surveillance, spying, and observation

## Note on Collecting, Reporting, and Analyzing Suspicious Incidents

DHS recognizes the increased vigilance of our industry and government partners, and encourages them to continually report suspicious activity and incidents. Effective information collection when a suspicious incident occurs enables faster and more thorough investigative follow-up. DHS recognizes that it is not always possible to gather detailed incident information, but collecting the following types of information will facilitate the investigative and analytic process:

- Date and time of incident
- Number of individuals involved
- Description of the incident, with a description of the business function of the facility involved
- Name and address of the facility
- For suspicious persons:
  - Name(s), aliases, including variations in spelling
  - Sex
  - Physical description
  - Social Security Number and any passport and visa information
  - Reason for being in the area or conducting the suspicious activity
  - Place of employment
  - Copy of picture ID(s)
- History of incidents of this kind involving this individual, especially at this facility

**For vehicles:**

- Make, model, year, color
- License plate and state
- Distinguishing marks, stickers, and embellishment on the vehicle
- Any history involving the same vehicle at this location or facility
- For aircraft: tail number and color scheme
- For boats: boat registration ID, color, and identifying information
- Description of suspect's surveillance equipment:
- Make and model of camera, binoculars, or recording equipment
- Subject and number of pictures taken
- Copy of pictures, if available
- Description of any other suspicious individuals in the nearby vicinity
- Contact information of the reporting individual, witnesses, and organization or facility
- Elements of local law enforcement or other local, State, or Federal agencies that have been notified
- Responsibility for follow-up actions
- Results of follow-up actions
- Points of contact for further information

## References:

Advanced Surveillance – The Complete Manual of Surveillance Training, Peter Jenkins, Intel Publishing, ISBN 0953537811, London, October 2003.

Air Force Office of Special Investigations Pamphlet 71-114, U.S. Air Force, 25 March 1996.

FAS - Federation of American Scientists  
1717 K St. NW, Suite 209, Washington,  
DC 20036, USA  
Tel: +001-(202)546-3300, Fax: +001-(202)675-1010  
E-mail: [webmaster@fas.org](mailto:webmaster@fas.org)  
Web: [www.fas.org](http://www.fas.org)

ICT – International Policy Institute for Counter Terrorism  
The Interdisciplinary Center Herzlia  
P.O.Box 167, Herzlia, 46150, Israel  
Fax: +972-9-9513073  
E-mail: [info@ict.org.il](mailto:info@ict.org.il)  
Web: [www.ict.org.il](http://www.ict.org.il)

Indicators and Warnings of Surveillance and Other Terrorist Operational Activity, Version 1.0, 06/2005  
Secret Service.

Institute for Conflict Management  
11, Talkatora Road, New Delhi 110001, India  
Tel: 91-11-2371 0374, Fax: 91-11-2371 5455  
E-mail: [icm@del3.vsnl.net.in](mailto:icm@del3.vsnl.net.in)  
Web: [www.satp.org](http://www.satp.org)

MI5 – United Kingdom Security Service  
The Enquiries Desk, PO Box 3255  
London SW1P 1AE  
United Kingdom  
Web: [www.mi5.gov.uk](http://www.mi5.gov.uk)

RAND - Research and Development  
1700 Main Street, P.O. Box 2138, Santa Monica,  
CA 90407-2138, USA  
Tel: +001-310-393-0411, Fax: +001-310-393-4818  
Web: [www.rand.org](http://www.rand.org)  
Terrorism Database: [www.rand.org/psj/rand-mipt.html](http://www.rand.org/psj/rand-mipt.html)  
The MIPT Database: <http://db.mipt.org>

SD Agent/The Surveillance Detection Manual, Dan Sommer  
ISBN 9979-60-950-8  
Iceland, 2004  
Secrets of Surveillance (A professional's guide to tailing subjects by vehicle, foot, airplane and public transportation)  
ACM IV Security Services  
Copyright 1993  
Gunbarrel Tech Center

Paladin Press  
7077 Winchester Circle  
Boulder Colorado, 80301  
1-303-443-7250

Shadowing and Surveillance  
A Complete Guidebook  
1986 by Loompanics Unlimited  
P.O. Box 1197  
Port Townsend, WA 98368

STRATFOR – Strategic Forecasting  
HQ, Austin, Texas, USA  
Tel: +001-(202) 429-1800  
E-mail: [service@stratfor.com](mailto:service@stratfor.com)  
Web: [www.stratfor.com](http://www.stratfor.com)

Surveillance Countermeasures (A serious guide to detecting, evading and eluding threats to personal privacy)  
ACM IV Security Services  
Copyright 2004, 2005 by ACM IV Security Services  
Gunbarrel Tech Center  
Paladin Press  
7077 Winchester Circle  
Boulder Colorado, 80301  
1-303-443-7250

Surveillance Detection-The Art Of Prevention  
Laura Clark  
William E. Algaier  
1663 Liberty Drive, Suite 200  
Bloomington , Indiana 47403  
Copyright 2005  
[WWW.AUTHORHOUSE.COM](http://WWW.AUTHORHOUSE.COM)  
800-839-8640

Surveillance Detection Management and Operations Field Guide, U.S. Department of State Diplomatic Security Service, Version 1.0, FY 2000 and Version 2.0, FY 2002.

Terrorism Research  
NSSC – National Security Studies Center  
NSSC, Mt. Carmel, Haifa 31905, Israel  
Tel: +972-4-8288145, Fax: +972-4-8288290  
E-mail: [nsc@univ.haifa.ac.il](mailto:nsc@univ.haifa.ac.il)  
Web: <http://nssc.haifa.ac.il/>  
TRC – Terrorism Research Center  
Northern Virginia, USA  
Tel: +001-877-635-0816  
E-mail: [trc@terrorism.com](mailto:trc@terrorism.com)  
Web: [www.terrorism.com](http://www.terrorism.com)



# Homeland Security

**DEPARTMENT of HOMELAND SECURITY**

**Surveillance Detection Training for  
Commercial Infrastructure Operators and Security**

***Aug/Sept 2006***

**ARMORGROUP**  
INTERNATIONAL TRAINING, INC.

