SURVEILLANCE AWARENESS

AIM: To have a basic understanding of surveillance, counter surveillance and anti surveillance methods

Intended Learning Outcome: By the end of this session trainees will be able to:

1. Describe the range of unwanted attention e.g. criminals, media, followers, stalkers, fixated persons
2. Understand the role of surveillance, counter surveillance and surveillance detection
3. Recognize surveillance detection techniques
4. Describe a range of basic surveillance techniques
5. Describe a range of anti-surveillance techniques
6. Explain the various technical aids that may be deployed by people or groups to assist them in surveillance
7. Explain what actions can be taken to counter unwanted surveillance

Teaching Methods

1. Visual presentations in the form of Power-Point will support the learning
2. Theoretical information will be provided in relevance to subjects covered
3. Practical scenarios will be undertaken by the trainee's.

National Occupational Standards:

PCP 2 – Plan and prepare to minimize threat and risk to Principals

PCP 4 – Establish and maintain secure environment

PCP 5 (SLP 2) – Communicate effectively in the workplace

PCP 6 – Maintain the safety and security of Principals whilst on foot

PCP 7 – Maintain the safety & security of the Principal whilst in transit

PCP 8 – Maintain protection whilst driving

PCP 12 – Maintain personal security awareness.

SURVEILLANCE AWARENESS

INTRODUCTION

"Surveillance is the (covert) observation of persons, vehicles, places or objects to obtain information on the activities and identities of individuals"

A planned attack is the final phase of a multi phase process that starts with target selection. This type of co-ordinated operation is normally directed at specific targets and involves an element of surveillance if they are to stand any chance of success.

SURVEILLANCE AWARENESS

Once a potential target or targets have been identified (phase 1), phase 2 involves a period of surveillance to establish the vulnerability of the intended victim

Lack of routine, surveillance awareness and good security procedures in general make it difficult for hostile surveillance to establish a pattern. This will involve having to spend more time in the target area that can result in compromise – the worst thing that can happen in a surveillance operation!.

Often in the wake of an incident and the subsequent investigation, it is frequently the case that activity associated with surveillance procedures was detected but not reported – or just as likely that reports were made but no follow up action was taken

Surveillance awareness training is essential to the overall effectiveness of a CPO and endeavours to make you aware of the following

1. ***Awareness of how a surveillance team operates***
2. ***How to spot hostile surveillance***
3. ***What measures can be employed to make a surveillance team's job more difficult***

NB: *Surveillance awareness will also enable you to conduct surveillance vulnerability assessments and counter-surveillance exercise as part of threat assessment.*

Reasons for Surveillance

Anyone planning an attack must mount some sort of surveillance activity in order to plan effectively. Surveillance activity is initiated to establish and identify as much information as possible about the subject

Whatever the motive, the aim is to try to gain as much information as possible along the following lines:.

The confirmation and identification of:

1. Subject's identity
2. Home address
3. Work address
4. Vehicles used
5. Family and associates
6. Other sources of information
7. Evaluate existing security
8. Evaluate subject awareness
9. Identify deliveries/services/visitors
10. Identify routines/patterns and predictable behavior
11. Identify the type of attack most likely to succeed.

Problems for surveillance

Terrorists and criminals are becoming increasingly professional and adept at surveillance. People with little training can easily employ readily available, sophisticated technical equipment.
However they also have constraints on their capabilities such as:

1.Limited time

2.Limited manpower

3.Limited logistics

4.Limited finances

Such limitations lead to repetition of the use of vehicles, operators and procedures in the target area. This repetition makes surveillance teams vulnerable to detection by "**AWARE PERSONNEL".**

The target; i.e. **You and/or your Client** are in control and surveillance teams are subject to the following problems:

1. ***Lack of support***
2. ***Boredom / daydreaming***
3. ***Paranoia and anxiety***
4. ***Vulnerability***
5. ***Orientation problem***
6. ***Staying alert***
7. ***Surveillance aware target***
8. ***Concealing equipment***
9. ***Cul-de-sacs/Dead-ends***
10. ***Bicycles***
11. ***Dress***
12. ***Public transport***
13. ***Over-exposure***
14. ***Other agencies***
15. ***Hostile environment/rough areas***
16. ***Third party awareness***
17. ***Poor communications.***

WHAT SHOULD YOU LOOK OUT FOR

UNWANTED ATTENTION Due to the Principal lifestyle i.e:

Film star, Footballer, Government Official, Royalty, Corporate executive etc; they are under threat from assassins, kidnap, low level criminals, stalkers, media, activist, lovers and terrorists

Hostile Surveillance Techniques / Tactics;

Surveillance can be a valuable and essential tool in a wide range of criminal activities. Assignment to this kind of duty requires that surveillance operative blend in with the environment. This almost always varies from case to case. Remember not everyone has had extensive surveillance training; however terrorists and hardened criminals are good at what they do.

Learn to respect them and learn surveillance techniques.

Here is an outline of the types of surveillance:

1. **Visual - Fixed Or Plant** Located in another building, normally able to see through windows or doorway

2. **Short-Term** Use's storefront or apartment

3. **Long-Term** Use's rooftop or rented dwelling

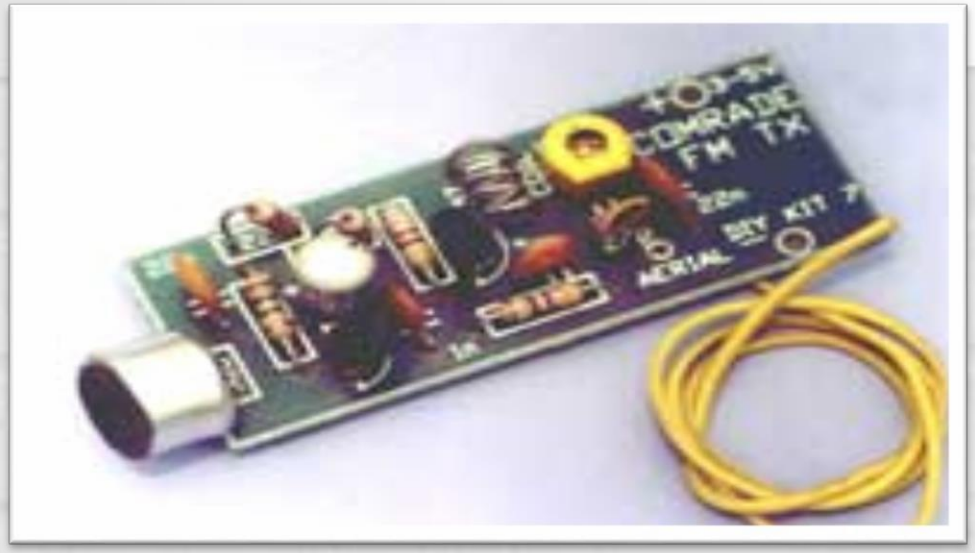
4. **Moving or Tail or Shadow**

5. **FOOT** Can be conducted by one to ten operatives

6. **VEHICLE** Could be using a number of vehicles use a tight tail in towns and cities and using a loose tail on motorways.

Audio or Electronic Eavesdropping

1.	**TELEPHONE**	line tap normally hard wired
2.	**PEN REGISTER**	This is a record of outgoing calls
3.	**“BUGGING"**	of premises
4.	**CONSENSUAL**	Using undercover tactic /accomplice / witness.



5. CONTACT - Not done very often. Usually for a piece of material being moved. Be aware of vendors, or other such people who would not arouse suspicion. Think about the Sky TV, electric company or the telephone repair van. Indoor posts, however; look for the use of equipment, such as spotting scopes, cameras, and recording devices.

6. VEHICLES used for surveillance will be as unobtrusive as possible. Aerials, communications gear, and other equipment will not be visible. Headlights will be wired separately so the car appears differently at night. In city traffic, handled by radio. This works well in both urban and rural areas.

The surveillance team make-up:

1.Size and composition (Typically 3 on foot / 4-5 in a car)

2.Equipment (personal and team)

3.Communications (personal and vehicle)

4.Vehicles.

Qualities of a good surveillance operator

He/She should be:

1. Confident
2. Quick thinking
3. Patient
4. Ability to blend in
5. Good eyesight and hearing
6. 6.Eye for detail
7. Awareness
8. Good memory
9. Good actor/bluffer
10. Good driver/navigator
11. Technically proficient
12. Robustly Fit.

Common Surveillance Methods

1. Static
2. Foot (Foxtrot)
3. Mobile (Vehicle)
4. Technical
5. Direct (making contact with the target)
6. Combination of the above

Basic Surveillance Terminology

1. Male subject is referred to as a	BRAVO
2. Female subject is referred to as an	ECHO
3. A building is referred to as an	ALPHA
4. A vehicle is referred to as a	CHARLIE.

Alert Calls

1. *‘STANDBY, STANDBY’*
2. *‘OUT, OUT’*
3. *‘GONE LEFT, LEFT’*
4. *‘GONE RIGHT, RIGHT’*
5. *‘STOP, STOP, STOP’.*

Control Calls

1. *Trigger'*
2. *'I have....(Eyeball / control)'*
3. *'Complete'*
4. *'Temporary unsighted'*
5. *'Unsighted'*
6. *'Wait'*
7. *'UKM / UKF'*
8. *'Cancel'*
9. *'Can you?'*
10. *'Backing / no longer backing'*
11. *'Committed'*
12. *'Foxtrot'*
13. *'Held'*
14. *'Intending'*
15. *'Look-alike'*
16. *'No deviation'*
17. *'Not one, not two' etc*
18. *'One up. Two up' etc*
19. *'180 (reciprocal) 20.'Tail end Charlie' 21.'Show red'*
22. *'Lift off/ Stand down'.*

THE THREE DISCIPLINES OF SURVEILLANCE

Surveillance is;

"The art of observing and/or following a subject, and cataloguing the meetings, stops and associates of the subject being followed"

The word means ***"Close Observation".*** Depending upon the quality of your enemy, this may be done individually or as a group and consists of "***Three Separate Disciplines":.***

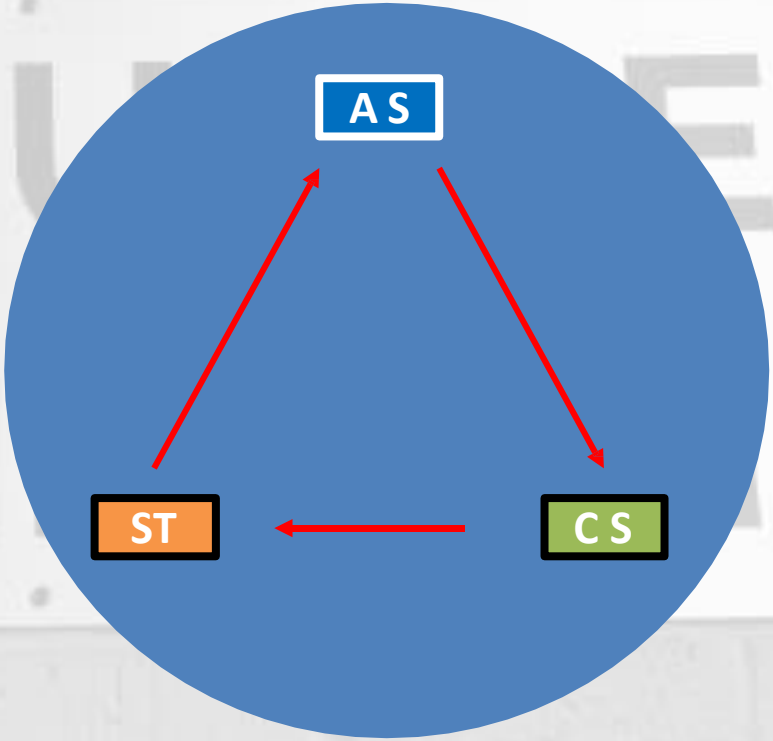
THE THREE DISCIPLINES OF SURVEILLANCE

THE PIECES OF THE PIE:

1. **ANTI SURVEILLANCE (AS)**

2. ***2.*** **COUNTER SURVEILLANCE (CS)**

3. ***3.*** **SURVEILLANCE TEAM (ST).**



ANTI-SURVEILLANCE:

- "The art of determining whether surveillance is being conducted on YOU through the incorporation of specific techniques without alerting those persons conducting the surveillance".

ANTI-SURVEILLANCE TECHNIQUES

Passive Anti-Surveillance;

Carried out at all times by the Protection Team, even if there is no reason to suspect that the enemy is mounting an attack against you. If the enemy is spotted, nothing is to be done initially. To alert them may possibly result in a quick attack

Active Anti-Surveillance;

This is where you overtly let the enemy know that you have discovered them; Making things obvious as in staring, talking to members of the public, **NOT THE PROTECTION TEAM** as they might not have spotted other members of the team.

Phases of Surveillance carried out by the enemy/criminals:

1. ***Target Selection/ Assessment - (Soft Phase)***
2. ***Operational/Attack Phase - (Hard Phase)***

SOFT (Target Selection/ Assessment)

1. Easiest to detect
2. Commit the most errors during this phase
3. Done by newer, less experienced terrorist group members
4. Done by amateurs with a “shopping list”
5. Generally continues for substantial time

HARD (Operational/Attack Phase)

1.A target has been selected 2.Better trained operatives take over 3.May include practice runs

4.May include photography and video.

SURVEILLANCE DETECTION:

In order for surveillance detection to be successful, a CPO will require detailed information regarding the opposition and their methods of operation. Information can be gathered through research, using the Internet, 'Who's Who', newspapers, TV etc. The primary source of information will be gained by mounting a surveillance operation. It is up to the CPO to pick up on the tell-tale signs. Females make excellent surveillance operatives as very few people expect females to do the job and they have natural and first-rate observation skills

Once surveillance has been identified, one can then develop a course of action that dissuades and demoralizes the surveyor so much that either surveillance is deemed too difficult, or manipulation of the surveyor can occur.

Three Basic Errors of Surveillance Teams:

1. ***CORRELATION***
2. ***COVER FOR ACTION***
3. ***COVER FOR STATUS***

1. **Correlation**—they do what you do
Example, ***"You stop, they stop".*** Their movements correlate to yours

2. **Cover for Action**—they don't do what they need to do in order to "fit in"
They don't blend in with their surroundings. e.g.; they are supposed to be pretending to be "lovers" in a car but are not interested in one another. They are not kissing, hugging, but are watching you

3. **Cover for Status**—they don't fit with their cover.
Example, they are supposed to be pretending to be fish salesmen but don't have any fish.

How Do You Detect These Errors?

1. Develop a Surveillance Detection Route (SDR) plan.
2. Use proper tactics along the SDR
   a)The Dangle
   b)The Natural Reverse
3. Solid coordination with CS Team

Surveillance Detection Routes (SDR)

1.Foundation of a surveillance detection plan

2.The basic building blocks are:

a)TIME

b)GEOGRAPHY

c)DISTANCE.

Time:

Most people don’t drive longer than 15 to 20 minutes “in-town”. With that in mind, make your surveillance detection route at least 30-45 minutes in duration

In other words, if you are conducting your surveillance detection route and you have been followed by the same vehicle for the last twenty minutes you should begin to wonder whether it’s surveillance.

Geography:

Incorporate different types of geographical locations along your route. These techniques can be a valuable security tool and can be easily adapted because they use the normal events and patterns in an individual's daily routine

For example, a route moving through these areas:

1. **Residential**
2. **Commercial**
3. **Educational**
4. **Industrial**

Why? Because it is highly unlikely that anyone following you through all these different areas is doing so by coincidence.

Distance:

Put mileage in your SDR! It “dovetails” with geography and time in ferreting out possible surveillance

Once you incorporate all three of these **(time, geography and distance)** into your SDR you can then begin to get a solid idea of those following you (coincidence or actual surveillance?).

TACTICS TO USE

1. THE DANGLE—IN a natural-looking manner, leaving something worthless (trash) behind on your route at a pre- arranged location and time

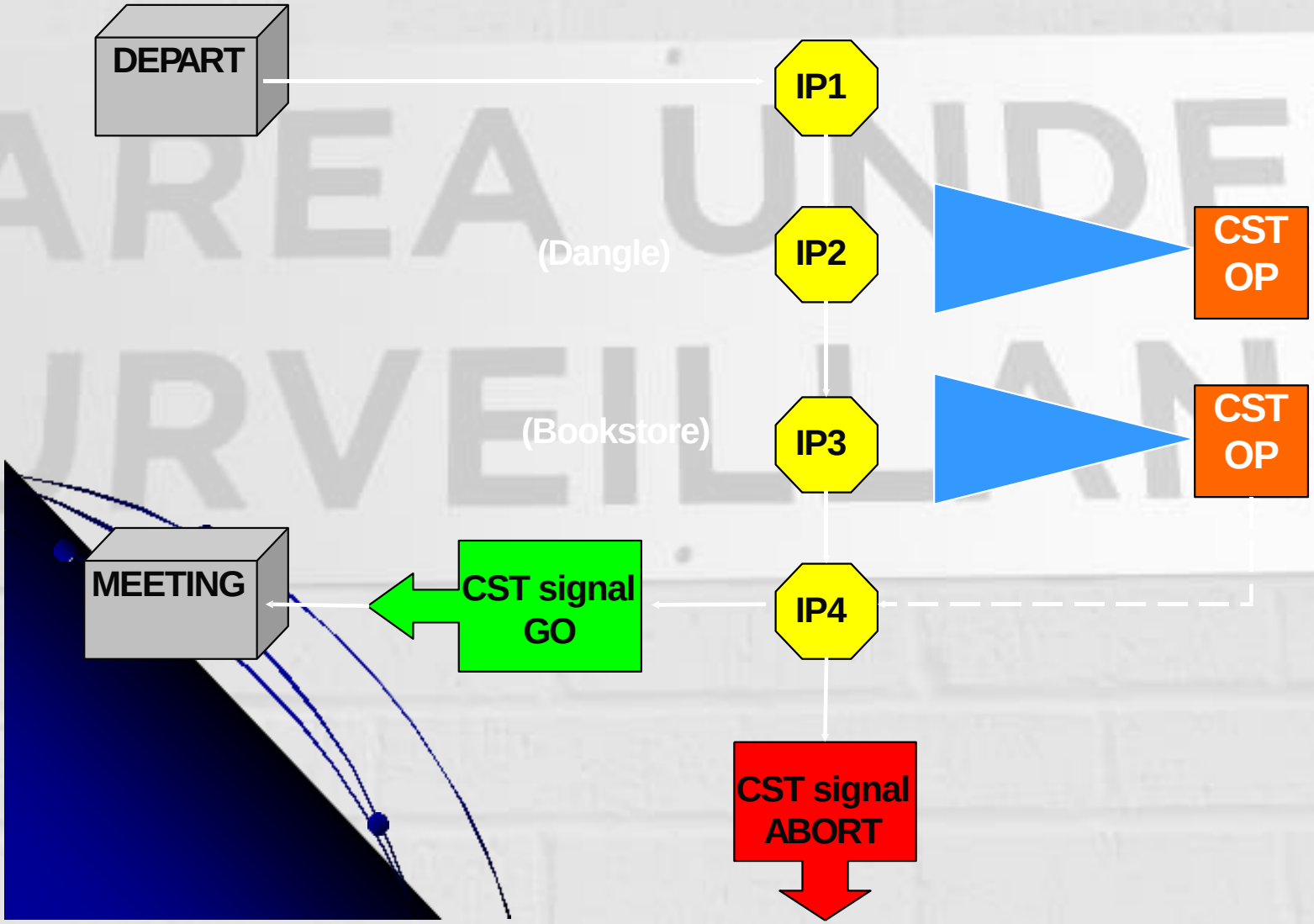
   Your Counter Surveillance Team (CST) observes the object you discard to see if a Surveillance Team (ST) picks it up

   Example: Man walks through a shopping mall to work every day. Every Tuesday and Thursday at 0900 he is to stop and buy a green carton of milk. He folds a napkin and slides it into the carton. He drops the carton on the ground next a specific bench and continues his route.

2.The Natural Reverse—in a natural-looking manner, as ascending escalators or stairs, turn and glance back down the steps

Not considered confrontational, as it’s a natural thing to do.

Sample SDR Flow



WHAT ARE THEY LOOKING FOR? ***WEAKNESS***

WEAKNESS!

Residence or Workplace

Terrain
Cover and concealment
Ingress and egress
Chokepoints

Routines
Deliveries
Peak traffic
Hours of operation
When you go to work
When you come home

Security Posture
Alert guards
Shift changes
Physical security
Alert personnel
Security detail in place

Response Forces
Weapons
Response time
Level of training.

WHAT SHOULD YOU LOOK FOR?

FORMS OF SURVEILLANCE:

One person on foot

Easier to detect (relatively)

Two people on foot

Harder to detect

Multiple vehicles

You're in big trouble still.

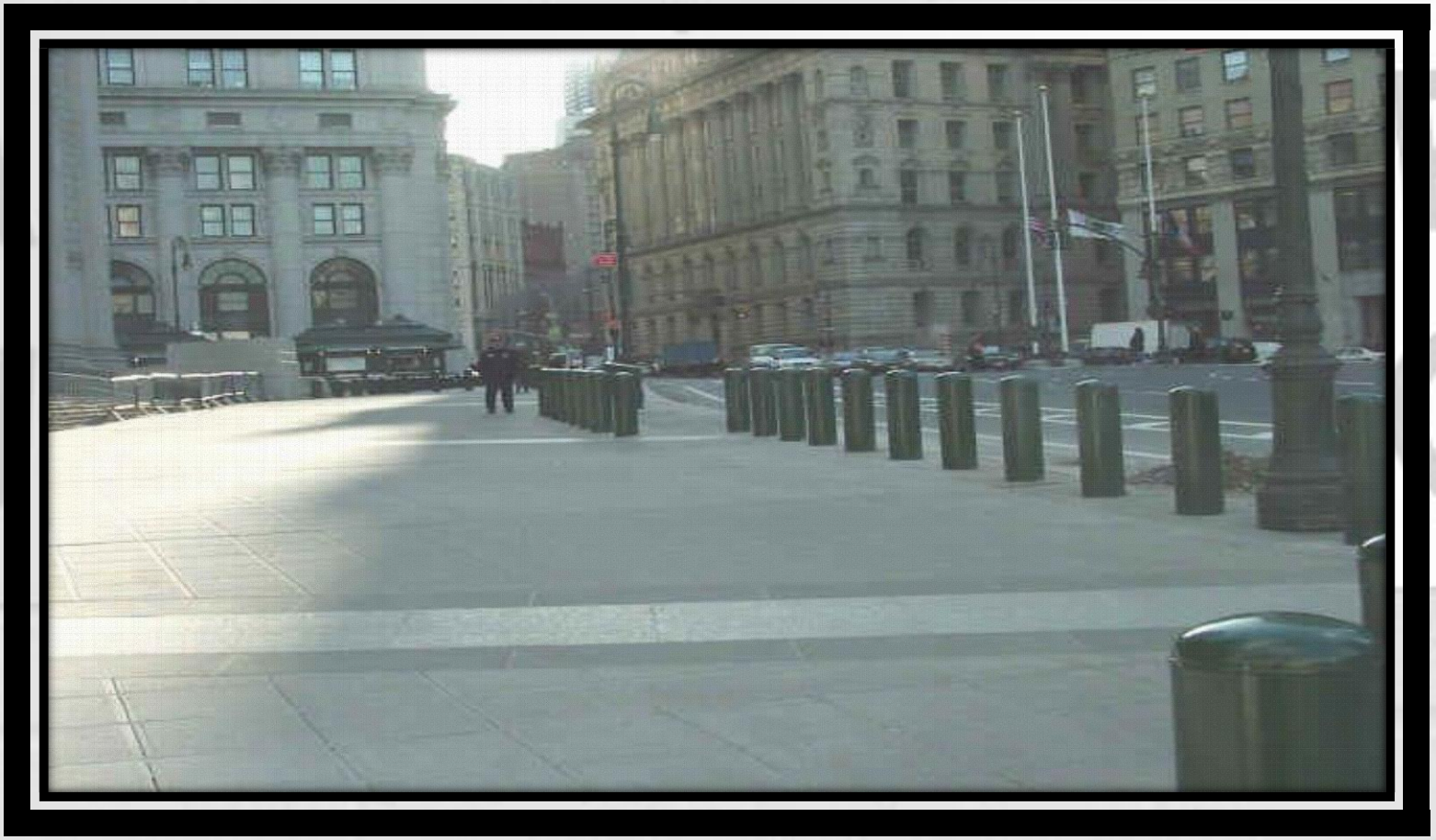
3 or more on foot with vehicular support

You're being followed by a national intelligence service or a well trained terrorist group…you're in big trouble now!!.

Stationary (this is the most common choice for terrorists)

DETECTING SURVEILLANCE

LEARN WHAT'S NORMAL.....



.....WATCH FOR CHANGES.

DETECTING SURVEILLANCE

SUSPICIOUS VEHICLES

Cruising the area
Not normal for area…they don't belong
Approaching residence or workplace and turning away
Breakdowns on or near residence or workplace or en route
Drivers who park one vehicle and leave in another
Parked vehicles
People sitting in cars
Unusual trucks and vans to many antennae
Commercial vehicles
Motorcycles
Scooters
Mopeds.

SUSPICIOUS PEOPLE

Loitering on or near your route to work/home

Road workers
Tradesmen
Construction
Bus stops
Joggers
Telephone booths

SUSPICIOUS CIRCUMSTANCES

People carrying parcels or packages that don't "look right"
Boxes, parcels, briefcases in unusual places
Bikes, mopeds parked in unusual places.

IF YOU SUSPECT SURVEILLANCE

Do you confront or not?

If you confront you destroy the chance to find out where the surveillant works…to which he reports…

It should be a decision taken by professionals on a "strategic" level

You can use a surveillant by giving "false" information to his bosses thru your actions that he observes and reports…

Bottom line…explain to the client that he MUST report any suspicious incidents to his security team…they will help him decide…!!.

LOSE, USE OR ABUSE?

Anti-surveillance is further defined as the actions or manoeuvres that a person carries out in order to:

1. ***To confirm that he is under surveillance and draw them into positions where you can identify the personnel/teams***

2. **To take appropriate evasive action once identified:**

    1.“LOSE” them
    2.“USE” them
    3.“ABUSE” them.

LOSE, USE OR ABUSE?

LOSE

Time a stoplight and slide through as it turns red
Hop the train/subway at last minute
Get on/off the elevator as the doors close
Drop in retail stores and exit the rear
Go into a mall and use one of the many exits
Personnel substitution
Vehicle substitution
Clothing switch-out (dark to light, hat-no-hat).

LOSE, USE OR ABUSE?

USE

Feed them “false” information via your actions

Have erratic departure and arrival times

Report to the wrong people/places

ABUSE

Run them ragged

Keep them up late by staying out

Get them up early

Keep them on their toes by leaving at odd times

Drive for long distances.

COUNTER-SURVEILLANCE

WHAT IS COUNTER-SURVEILLANCE?

"The art of determining whether surveillance is being conducted on OTHERS through the incorporation of a TEAM using specific techniques without alerting those persons conducting the surveillance on the target"

NB: These actions are normally pre-planned and rehearsed by the team or individual

Basically Counter-Surveillance is when every member of the team is trying to:

1. ***Identify any presence of a hostile surveillance team***
2. ***Prevent that a person (Principal) being under surveillance.***

COUNTER SURVEILLANCE MEASURES

Method of Operation deployed by hostile surveillance teams (Foot / Mobile)

There are four basic phases of Surveillance:

1. ***START POINT***
2. ***TRIGGER (PLOT-UP OR STAKE-OUT) PHASE***
3. ***PICK-UP & FOLLOW PHASE***
4. ***HOUSING PHASE.***

1. START POINT

Surveillance must begin by observing a location where the subject is known to frequent or inhabit such as:

1.Subject's residence 2.Place of

work 3.Publicised event/venue

4.Airport / Railway Station / Ferry etc 5.Other

frequented locations.

2. THE TRIGGER (PLOT-UP & STAKE-OUT) PHASE;

The start point is where the trigger is mounted; the trigger initiates any subsequent monitoring of the subject movement. A trigger could be any of the following:

1. ***Observation Post (OP)***
2. ***Vehicle***
3. ***Technical***
4. ***Inside information***
5. ***Walk / drive past***

Stake-Out (Methods):

1. ***Primary***: Trigger and Box
2. ***Secondary***: No direct trigger and tight box with occasional drive/ walk pasts
3. ***Tertiary:*** No trigger and a loose box / frequent walk / drive pasts.

Considerations when holding trigger

1. Not in 10-2 observation arc when subject exits start point (In peripheral vision
2. Length of time in position (exposure)
3. Communications with team
4. Trigger should not ***'TAKE' (i.e.Not follow the subject)***
5. Aware of direction subject might take
6. In a position to see the direction that the subject takes
7. Positive ID of subject
8. Awareness of alternative exits the subject might take
9. Act natural (reason to be there)
10. Have a cover story if queried / challenged
11. Must be able to positively ID trigger & subject
12. No interrupted views.

Defensive Measures

1. Make use of a scanner, which constantly scans the VHF and UHF commercial wavelengths in order to pick up close transmissions, which may be used by surveillance teams
2. Use encrypted communications amongst the Close Protection Team in the event a Surveillance Team is monitoring for your transmissions
3. Carry out a foot patrol and a mobile patrol of the Principal's residence in order to look for any likely trigger positions that a surveillance team may use. Remember the various means a trigger can be performed and the trigger locations open to them
4. Search for anything unusual such as people sat about in vehicles or on a motorbike, make note of empty vehicles and their contents, things to look for are: briefing sheets, Radios, Maps, Fast food wrappers and old newspapers.

Defensive Measures

5. Approach and confront anyone you find suspicious.
6. Widen your search area and check along known and frequent routes paying attention to choke points for trigger locations away from the starting point
7. Have a member of the team depart in the Principal's vehicle as a decoy in order to draw the surveillance into the open.
8. Utilise one of several vehicles with tinted glass in order to transport your Principal. The watchers will be unable to identify which one contains the Principal
9. Vary times of departure***.DO NOT SET A ROUTINE!***
10. Watch for vehicle pulling out behind you, (only an amateur will do this).

3. PICK-UP & FOLLOW-PHASE;

If the target is surveillance aware this is a very difficult phase for the hostile surveillance team / operator without considerable resources in terms of trained manpower, vehicles and communications

Considerations:

1.Urban environment
2.Rural environment
3.Motorways
4.Lane changes
5.Speed
6.Accurate reporting
7.Communications
8.Handovers at roundabouts
9.Lost communications
10.Orientation
11.Appearance changes and exposure.

Defensive Measures

1. During the follow phase the Protective Team should throw a cordon around the Principal's vehicle. These operators should be looking out for anything unusual or frequent sightings of the vehicles

2. The Principal or driver should carry out these manoeuvres as previously described concerning anti-surveillance. e.g;

    i. Park walk, bench stop and dangle
    ii. Overpass
    iii. Natural Reverse going up escalator and CST posted to observe escalator traffic
    iv. "Stake Out" locations on choke points (home, work, key intersections)

3. The route the Principal takes should be varied as should be the timings

4. Drive a circuitous route making at least three turns in directions to the left or right so that you box three sides to a square, anyone also seen taking the same route should be treated with caution.

4. HOUSING-PHASE (STOPS)

The hostile surveillance will be looking for:

1. Address
2. Description of building
3. Anything carried / handed over?
4. Reaction (greeted?)
5. How subject enters (knock & wait / own key)

NB: *the Housing is now the new start point and the process starts again*

Defensive Measures

1. The SAP team should arrive at the destination prior to the Principal and check for watchers who are already present and for those that may have followed the Principal.
2. Take the Principal into a controlled area where he/she has easy and safe access and it would be difficult for a surveillance team to enter.