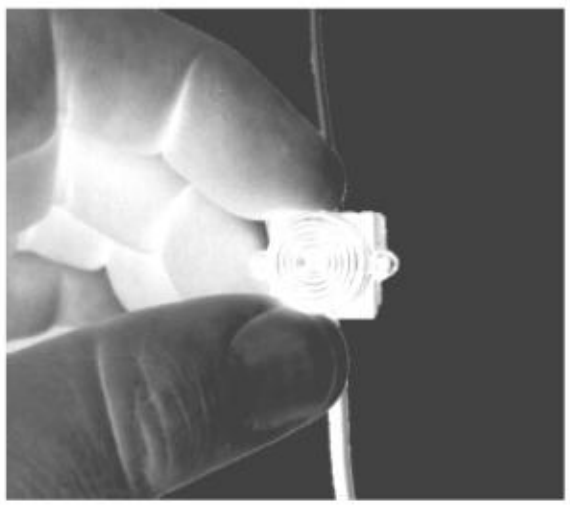
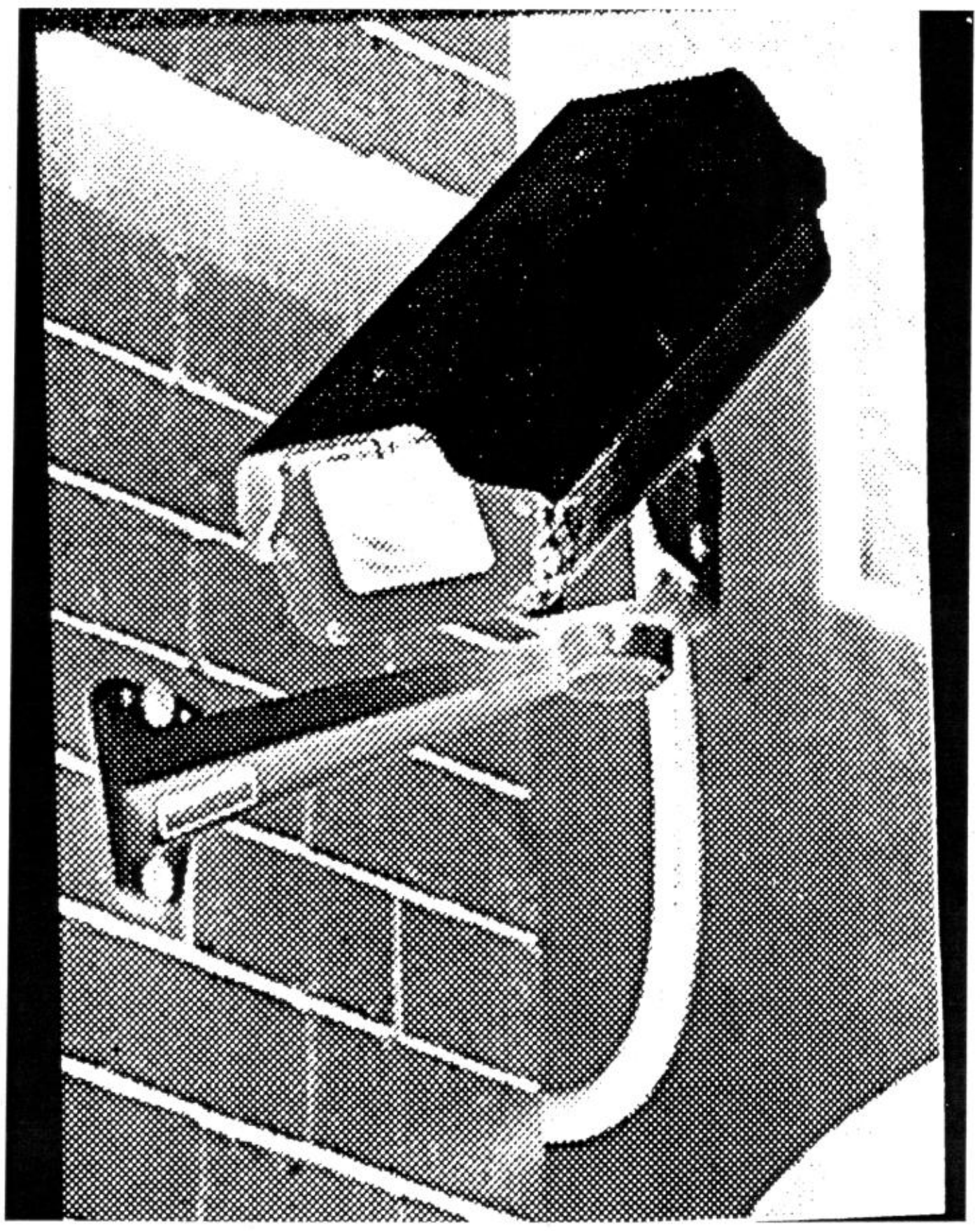
# Security & Counter-Surveillance

## Information Against the Police State





**Revised & Updated:**
***New*** Surveillance Technology & Techniques
***New*** Section on Informant & Infiltration Operations

# Contents

2009 edition; Vancouver, Canada/Coast Salish Territory



"Those in authority fear the mask for their power partly resides in identifying, stamping and cataloguing: in knowing who you are... our masks are not to conceal our identity but to reveal it..."

Text on inside of 9,000 masks distributed at the Carnival Against Capitalism, London, June 1999

## Big Brother is watching, more than ever before

In countless ways, surveillance is emerging as the dominant way the modern world organizes itself.

Britain now has an estimated 4.2 million CCTV cameras—one for every 14 citizens. People in central London are now caught on camera about 300 times a day.

Surveillance is a condition of modernity, integral to the development of the nation-state and capitalism...

More than ever before, our lives are visible to others, from government agencies and security services to the owners of the websites we surf and the stores where we shop. They track us in public, in workplaces and online, compiling our personal information in massive databases and sorting us into categories of risk, value and trustworthiness.

CCTV cameras are just one of their tools. Others include radio frequency identification (RFID) chips, GPS location trackers, website cookies, facial recognition software and store loyalty cards. Computer programs used by security services can monitor and analyze billions of phone calls and e-mails in real time. We even make it easier for our trackers by willingly disclosing pieces of our lives on social networking sites like Facebook or in online contests & questionnaires.

In one form or another, surveillance has always been a part of human society. What's new is computer technology that has made it possible to integrate vast and diverse bits of information. As well, our post-9/11 obsession with eliminating risk has produced an architecture of mass surveillance in which everyone is treated as a suspect.

Don Butler, "Big Brother is watching, more than ever before", *Vancouver Sun*, Feb. 3, 2009

*And for those who really are 'suspects', read on...*

# 1. Introduction

Security is vital to the success & survival of the resistance movement. This is because we have an enemy who actively works to undermine, neutralize, & ultimately destroy us. Failure to remain aware of security concerns can mean the difference between victory or defeat, freedom or imprisonment, life or death. Not only for yourself, but others around you.

Information gathered from various sources, & that is subjected to analysis & comparison, is called **intelligence**. The gathering of intelligence is a vital part of counter-insurgency operations, without which the enemy does not know who, what, where or when to strike.

Security & Counter-Surveillance measures are designed to limit & deny the flow of information to enemy forces. It is based on the principle that counter-insurgency is a permanent part of society and that those engaged in resistance are always vulnerable to surveillance & repression.

# 2. Surveillance

**Surveillance** is the continuous, secretive observation of persons, places, things or objects, in order to gain information.

**There are two types of surveillance: physical & technical.**

**Physical surveillance** is carried out by enemy personnel on foot and/or by vehicle. It is the only way a target person can be continuously observed over an extended period of time. Surveillance teams can be comprised of two persons in one vehicle, or a dozen operators in six vehicles (or even more, of course). In addition, motorcycles, bikes, planes & helicopters may also be used.

In this category we must also consider informants, infiltrators & collaborators. They may be police agents, civilians recruited by police, or former comrades. This form of physical surveillance is the main source of intelligence on people's thoughts, plans & activities. It is sometimes referred to as 'human intelligence'. Because of the sensitive nature of personal information they are able to gather, and their ability to influence events, infiltrators & informants are especially dangerous.

**Technical surveillance** is far more common. With widespread use of telecommunications (phone, cell, pager, internet, fax), technical surveillance is a main source of intelligence on a person's day to day activities, contacts, personal relationships, etc. More generally, it consists of technical devices to record, document or monitor a target individual's movements, conversations, or activities. This includes listening devices in homes & cars, tapped telephones, monitoring of internet activity, CCTV video, tracking devices, night-vision devices, etc.

The urban environment is far more conducive to surveillance, due to the large masses of people, communications & electrical systems, structures, & vehicles in which operators & devices can be concealed. In the city, there are also tens of thousands of CCTV video cameras, in stores, banks, malls, offices, schools, transit, streets & intersections.

In rural areas, physical surveillance is more often necessary due to the lack of telecommunications, roads, etc. Low population densities also serve to identify surveillance operators as 'outsiders'. For these reasons, physical surveillance in rural areas often requires long-range observation (by ground teams, aircraft, or satellite in high priority situations). In some cases, police in military-style camouflage secretly conduct surveillance at a much closer range.

# 3. Security

**Security** *n.* 1. Measures adopted to guard against attack, theft or disclosure. 2. Something that gives or assures safety & confidence…

As noted, the purpose of security is to protect our movement. A vital part of this is to limit or deny the flow of information to enemy forces. The following 4 principles should be seen as basic & fundamental security guidelines:

1. **Do not send or discuss sensitive information over any form of telecommunications** (phone, cell, internet, etc.), all of which are vulnerable to interception. **Cell Phones** can be made into active listening devices and should have their batteries removed before discussing any secret information.
2. **Never discuss sensitive information in any enclosed area** vulnerable to listening devices (i.e., homes, vehicles, cafes, etc.).
3. **Follow the *Need-to-Know-Only* Rule:** If a person is not involved in the information, then they do not need to know its contents. The less a person knows, the less danger there is they can tell others.
4. **Avoid those unable to follow basic security codes.** They are a danger to you and the movement. This includes persons who talk too much, who do not take security seriously, alcoholics, etc.

# 4. Principles of Surveillance

As noted, surveillance is the secretive, continuous watching of a person, place, vehicle, or object in order to gain information. In order to be effective, surveillance must go unnoticed and be undetected. As soon as the target is aware he/she is under surveillance, they will alter their behavior & conceal any 'suspicious' activities, as well as stop the flow of information. For this reason, surveillance can be difficult to detect because it strives to be covert & hidden.

Developing information through surveillance is a progressive & often lengthy process. It is from many pieces of information that an overall picture of the target's patterns is developed.

Surveillance will normally begin with limited information on a targeted individual's activities, a residence or workplace, etc. More info will be developed in order to identify times, locations, routes of travel, or activities on which

to focus the surveillance effort (referred to as a **target pattern analysis**).

The more extensive the surveillance effort, the greater the amount of intelligence produced. The extent of surveillance depends upon the importance placed on the target by police-intelligence, and the target's expected level of awareness & counter-surveillance knowledge (soft target vs. hard target). Just reading this manual can make you a harder target.

Because of the resources & capabilities of our enemy, and its intent to monitor & repress rebellious tendencies (of which we must assume we are a part of), surveillance against our movements must always be considered as being possible (if not probable).

# 5. Physical Surveillance

Physical surveillance is carried out by enemy personnel (operators) on foot and/or by vehicle. It is the only way a target person can be continuously observed over an extended period of time. On foot or in a vehicle, operators must keep their surveillance target in sight. A team assigned to maintain this line-of-sight is said to have '**command**' of the target. In order to avoid detection, the command is frequently shifted, so that no one operator or team is in direct sight of the target for too long a time (**shifting command**).

Sophisticated surveillance efforts can involve many different operators & vehicles. In such cases, teams are deployed all around the target in a '**floating box**' (in front, the back, sides, and on parallel routes).

If physical surveillance is being carried out, then it can be assumed that technical surveillance is also occurring, and may have been for some time before physical surveillance began. This is because physical surveillance requires multiple operators if it is to be succesful, and can be draining on personnel and resources. It's therefore possible that surveillance operators may have access to audio recordings of the target's conversations in a residence or vehicle, while they are observing them.

## Surveillance Operators & Vehicles

Surveillance operators can be of any race, ethnicity, size, shape, etc., wearing any style of clothing, listening to any type of music, etc. Not only are police & intelligence agents used, so too are civilians & family members. They can be men, women, youth, or elders (i.e., the RCMP's 'Watchers' of the early 1980s). Likewise, vehicles used by surveillance teams can be of any model, year, condition, colour, etc. Appearance by itself will rarely reveal a sophisticated surveillance effort. Instead, it is their activities which must be observed.

In order to coordinate the efforts of many team members, communications body gear is worn by operators. This usually consists of clear, plastic earpieces placed in one ear, and microphones attached to jackets or shirts at chest level or in collars. A volume, on/off switch or device may be contained in a pocket. Variants of this include cell phones with ear and mic attachments, MP3 players or iPods, etc. The proliferation of these devices can make it very difficult to identify surveillance operators based simply on the fact that they are plugged into some kind of device.

## Fixed Surveillance

Fixed surveillance (meaning it doesn't move) is set up around a target's home, a business, etc., to observe activities, patterns of movement, associations, or even to begin surveillance of a target expected to appear at the location (*stakeout*). Another term for a fixed surveillance position is **Observation Post (OP)**.

It is usually conducted from overlooking positions such as hills, buildings, apartments, or vehicles parked in the area. Fixed surveillance can change into mobile surveillance with operators pre-positioned and ready to follow.

****

**Rural:** In a rural area, fixed surveillance can consist of an armed reconnaissance team (police or military) taking up positions from which it can observe the target location. Because this type of surveillance requires special fieldcraft skills (i.e., camouflage), it is most often conducted by specially trained police or military units. Another factor is the greater likelihood of firearms in rural areas (hunting rifles).

Teams may set up OPs on overlooking hills or mountainsides, using hi-powered long-range cameras & telescopes, or in nearby forest, abandoned buildings, fields, bushes, etc. Operators may wear camouflage clothing, including 'ghillie suits', and construct camouflaged hide positions (digging out an area large enough to lie in, setting up overhead support, and covering it with the top layer of earth).

## Mobile Surveillance

Once a target person has been observed and is leaving the location, the surveillance then becomes *mobile*. On foot or by vehicle, the target is followed until he/she stops. A surveillance box is again set up with one operator having direct line of sight on the vehicle or location (this is the **trigger**, who alerts other operators as to actions of target).

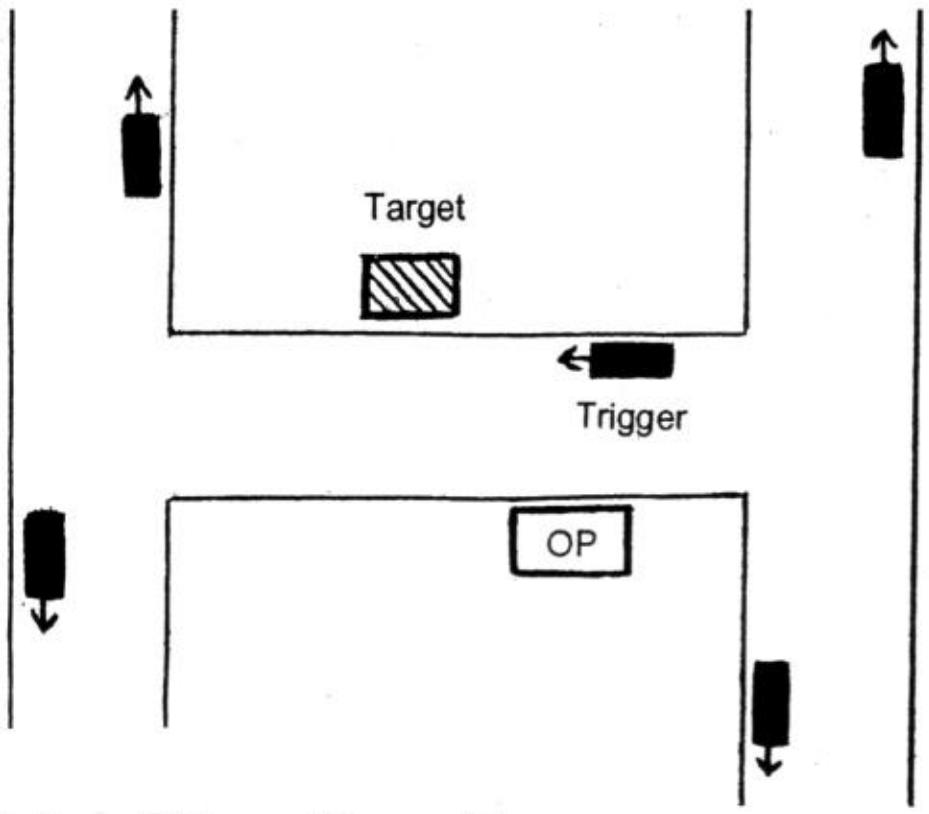
As the targeted individual re-appears on the move, the fixed surveillance box again transitions to a mobile surveillance. In high-priority cases, the surveillance box will cover all known routes in and out of an area and can literally surround the target.

If a person drives, stops and walks around, surveillance vehicles will also drop off foot operators. They will then position themselves in a box around the target's vehicle, or assist in the foot surveillance by picking up and dropping off operators.

For their part, foot operators may change jackets, hats, and other items of clothing in order to avoid detection. Once detected, they will be removed from the operation and replaced. Operators may also use bicycles if the target moves by bike or foot.

**Rural:** mobile vehicle surveillance in rural areas presents some problems to operators due to the lack of cover on roads.. Aerial surveillance can greatly assist, as can GPS tracking devices (although they cannot say for certain who drove the vehicle without some form of line of sight observation). Nevertheless, rural mobile surveillance will follow these basic patterns, with some modifications.

## Four Phases of Mobile Surveillance (foot and/or vehicle)




**Stakeout/Surveillance Box**

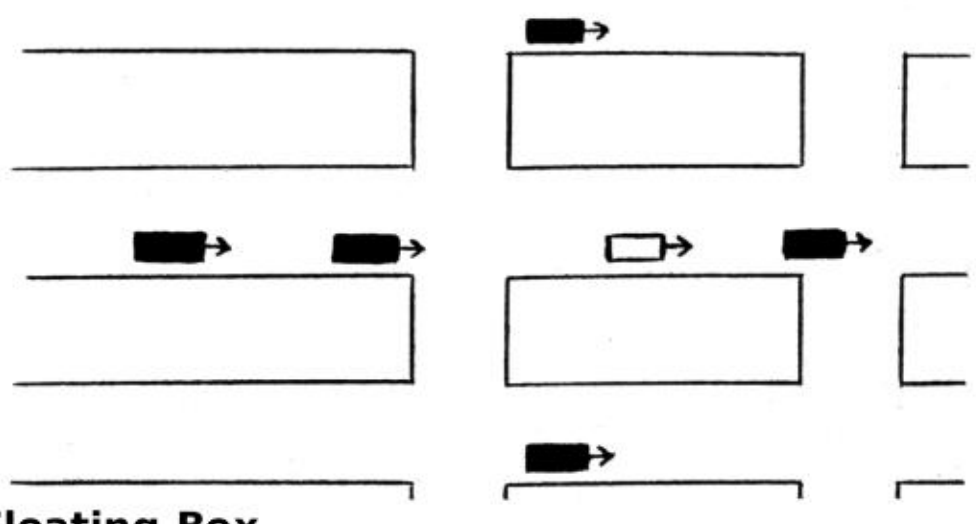
**1. Stakeout:** surveillance team members are pre-positioned in a specific area, usually in a box to cover all routes of travel in/out. It may be a target's residence or a location to which the target is expected to visit.

A stakeout can involve Observation Posts (OP's). In urban areas this could be overlooking apartments or houses, vehicles parked in the street, etc. An OP limits possibility of detection over a long period of time.

**2. Pick-up:** occurs when the surveillance team establishes command of the target entering and then leaving the area.

**3. Follow:** begins immediately after the pick-up. This phase covers all aspects of surveillance while target moves from one location to the next.

**4. Surveillance Box:** begins as soon as the target stops at another location. A standard surveillance box covers all routes in/out of a specified area. The main difference between a stakeout & a surveillance box is that in a *stakeout*, it is anticipated that the target will appear. In a surveillance box, it is known that the target is in a specific area or location.



**Floating Box**

## Other Forms of Physical Surveillance

**Mail:** although not used as much as email, police and intelligence agencies have a long history of intercepting postal deliveries, including letters and packages. Agents can gain authorization to intercept mail, which is then delayed from delivery while they open it, check the contents, and then re-seal it. It is not a secure form of communications or transporting items.

**Garbage:** going through people's personal trash is a common practise used by police, intelligence, and private investigators. This includes old notes, letters, bills, invoices, receipts, flyers, prescriptions, drawings, etc., all of which can provide personal or business information. Garbage can also be a source of forensic evidence (residue, chemicals, bodily fluids, hair, etc.).

**Neighborhood Watch/Vigilante Citizens:** these entities often have direct contact with police through neighborhood watch groups or community policing centres. They should be considered a form of physical surveillance in that they can report any observations they have made of you, your activities, friends, etc. They may also help provide police with residences or businesses to use for surveillance.

# 6. Technical Surveillance

As noted, technical surveillance is the use of devices or technologies to monitor and/or record the activities of a target. Today, technical surveillance is widespread in society, due to the ongoing development of new technologies and equipment.

### Telecommunications

Phones, cells, Internet, fax, and pager are especially vulnerable to surveillance due to their control by government & corporations, and the use of computerized digital technology in telecommunications systems. This allows for greater access, storage, retrieval and analysis of communications, without the need for physical access to a residence or workplace.

**Telephones:** Telephones can be made into active listening devices through a technique known as a hook switch bypass, even when not in use. Cellular & cordless phones are among the least secure forms of communication as they can be intercepted by commercially available scanners.

**Cell Phones:** Cell phones, because they operate through satellite & transmission tower networks, can be used to track a person's movements & location. Cell phones can also be made into active listening devices, even when not in use. Many also have built-in digital cameras and video capability. The proliferation of cell phones and their capabilities greatly expands the potential for surveillance, while reducing the visibility of the operator with a camera (or communciations device).

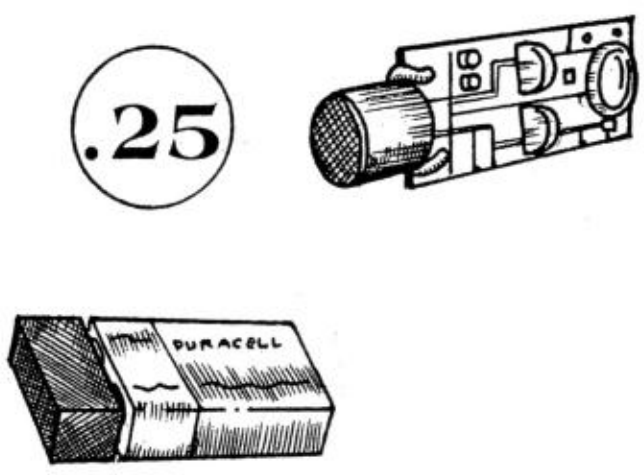
**Internet & Computer:** Like cell phones, the Internet is a very insecure form of communications. Emails you send, or web sites you visit on your personal computer, can be intercepted just like a phone call. If your computer is ever seized or stolen by police, they can access large amounts of data (i.e., emails, website visits, documents, photos) even if you have deleted it. This is because instead of actually deleting

items, your computer's hard drive only overwrites data as it needs to. Keystroke loggers can be installed on computers, enabling surveillance to read everything you've typed. In addition, when you are online with your computer, software programs can be covertly downloaded onto your computer that enable another computer to access it and gather information.

Anytime you go online to check your email, that location can be traced through Internet Protocol (IP) addresses. The FBI have a program they can download to your computer via email that provides access to your internet activity. These methods have been used to arrest people making internet threats. In some cases, police identify an IP address then acquire video surveillance of the suspect posting new threats. Police also commonly check people's Facebook accounts and similar sites for incriminating text, photos or video.

## Listening Devices

Audio surveillance is one of the main methods of recording conversations for both intelligence gathering as well as criminal charges. In fact, multi-million dollar investigations and trials are often based almost entirely on recorded conversations (people caught making incriminating statements to either undercover cops or informants).




*Two commercially available wireless listening devices;* the top one can be wired to a battery or electrical source in the residence/vehicle. The bottom one is connected to a 9V battery.

Listening devices, also known as **bugs**, are usually small microphones attached to a transmitter & an energy source that are placed in a residence, workplace, vehicle, etc. They can be as small as 1.5" x 1". They transmit to a receiver, which is usually in the area (i.e., a nearby observation post/vehicle). The proximity of the receiver will depend on the effective range of the device. In some cases, police have used planes to receive transmissions when it wasn't possible to get a ground vehicle close enough to a hidden transmitter (worn by an informant). Buildings and heavy traffic can disrupt transmissions, depending on the device. At times, police have to use abandoned buildings, rooftops, or other areas while posing as workers in order to receive transmissions from a device.

The most common listening devices are **wireless** and transmit to a nearby receiver using radio frequencies. They must have an energy source. In sophisticated devices, small but powerful batteries are used that can last months. In cheaper models, battery packs are strapped together and hidden along with the mic. Of course, the larger, bulkier battery packs are more easily detected and must sooner or later be replaced with fresh batteries. Devices can also be wired to household or vehicle energy sources.

Another type of listening device is the **wired** mic, in which a wire runs from the mic directly to the receiver, usually in a nearby room/apartment. Wired microphones do not need an energy source as they are powered by the monitor through the wire. Wired mics have a better sound quality but are not as commonly used today due to their greater potential for being discovered (via the wire).

Listening devices are placed in areas where conversations usually occur, i.e., living rooms, kitchen, bedrooms, and vehicles. They can be hidden in wall sockets, light switches, lamps, behind paintings, in ceilings, walls, air vents, etc. In high-level operations, devices have also been placed in park benches & cafes frequented by the target.

Although scanners & other specialized equipment can be used to locate devices, this does not ensure areas are secure. New technologies can overcome such detection devices, and 'bugs' can be remotely turned off, temporarily cutting any RF transmissions. The money & effort spent acquiring such gear will only alert the surveillance team.

**As a general rule, all enclosed spaces should be considered vulnerable to surveillance by listening devices, especially those used or frequented by movement members/ associates, etc.**


A listening device is contained in this watch.

Another type of listening device is that worn on the body by an informant or infiltrator. Like other types of devices, it will have a small concealable microphone attached to a transmitter & battery. More sophisticated listening devices can also be concealed in any number of objects (cameras, pens, watches, bags, cups, etc.). Listening devices used by the FBI & ATF in undercover operations against biker gangs were hidden in pagers and cell phone batteries. They had on/off switches so they could be turned off if there was a scanner being used to detect hidden transmitters.

Laser devices are also used to collect window vibrations and convert them into audio signals, thereby recording conversations in offices, apartments, etc.

## Parabolic Microphones

Powerful microphones are designed to eavesdrop on conversations over a long distance. Also referred to as a 'bionic ear', parabolic mics are hand-held devices usually with a boom mic and a round disc attached. The operator wears ear-phones. Some parabolic mics have effective ranges of 300 metres. Civilian versions are sold for hunting, and some attach to binoculars (which will have a small boom mic sticking out).

## Video Cameras

Closed-circuit television (CCTV) is one of the most widespread examples of technical surveillance in society. In every city there are tens of thousands of CCTV video cameras, in stores, banks, malls, offices, schools, transit, streets & intersections.

Mini-CCTV camera

For surveillance operations, miniature CCTV video cameras are also routinely used. They have filmed people making and selling drugs, weapons, & bombs, as well as making incriminating statements. Mini-CCTV cameras can be as small as a dime in diameter (with a small pin-hole aperture). Like listening devices, mini-video cameras can be hidden in almost anything, inc. a pager, a teddy bear, a VCR, a clock, a radio, a smoke detector, etc. (such devices are available on the commercial market). In apartments or motel rooms, or any adjoining structures, surveillance teams can gain access and drill a pin-hole through walls, ceilings or floors, and insert a pin-hole camera (as is done during barricaded suspect situations).

Mini-CCTV devices must have a power source & a transmitter to relay the information to a nearby monitor—the surveillance team (or recorder). Like a listending device, the power source may be a battery or it may be directly wired to a residence or vehicle power supply. Sophisticated video cameras also have night-vision.

In cases where physical surveillance of a suspect was either too difficult, or illegal activities occurred at too long an interval, mini-CCTV video cameras have been covertly set up outside a residence. They are motion-sensitive and only record data when there is movement. In Germany 2007 this technique was reportedly used to monitor the homes of persons suspected of carrying out sporadic attacks over the course of several months (i.e., when physical surveillance would be largely unproductive).

Powerful video cameras are also mounted on helicopters, planes and Unmanned Aerial Vehicles (UAV). These vehicles can hover or circle an area at very high altitudes, virtually out of sight and sound range, and still identify an individual's face.

Many cell phones and digital cameras now have video capability. More police forces mount video cameras in their cars. In 2007, UK police adapted a head-mounted mini-camera that can be worn by uniformed officers to record incidents & suspects. It resembles a small flashlight. There are also new shoulder-radios used by some police forces that have mini-video & photo cameras in them.

## Still Photography

The use of 35mm camera & digital cameras remains an important tool in surveillance work. It is especially useful for documenting & identifying individuals, locations, vehicles, etc. In particular, 35mm film and hi-quality digital cameras provide sharp, clear pictures as opposed to images taken from a video. Photographs must be taken by an operator with line of sight observation of the target. With hi-powered zoom lenses, close-ups can be achieved over great distances.

Many cell phones now have digital cameras installed and can be used to take photos of persons, license plates, documents, etc.

## Tracking Devices

Usually attached to the rear underside of vehicles, these devices emit a signal which can be tracked by satellite & cellular technology (the global positioning system: GPS). Any vehicles equipped with GPS technology are already capable of being tracked (i.e., the OnStar network). As noted, cell phones are also tracking devices.

One documented version of a tracking device used by the FBI consists of a GPS transmitter, a cellular antennae, a battery pack, and a component box. These were encased in black metal boxes, connected by wires, and attached to the underside of vehicles by extremely strong magnets. The battery pack, containing 4 lithium D-size batteries, was a cylindrical metal tube 12 " long. The component box was the size of a paperback book. With this, the location of a device could be determined within a few yards.

ProScout tracking device (bible sized)

Commercially-available tracking devices, such as the Quicktrack GPS Tracker, consist of a one black metal box with strong magnets. It is 4.6" by 2.5" in size and has a battery life of 40 hours in tracker mode, and one month in standby.

Recent GPS devices available on the commercial market are almost as small as a wristwatch. Sophisticated tracking devices can be installed anywhere on a vehicle (not just the undercarriage, this is especially true if the vehicle is impounded or left for long periods unattended).

— AP

**OK for medical chip**

The U.S. Food and Drug Administration has given approval to Applied Digital Solutions of Delray Beach, Fla., to market the VeriChip, an implantable computer chip about the size of a grain of rice, for medical purposes. The chip could hold a person's entire medical history.

A variant of tracking devices is the Radio Frequency ID (RFID), a small device (as small as a grain of rice) that emits a signal. It is used by corporations to track the shipment of goods and to prevent shoplifting. Miniature RFID's are surgically implanted in the skin of persons for medical reasons (it contains their medical history) as well as for security (potential victims of kidnapping). The FBI has also used RFID and GPS devices to track the shipment of drugs.

## Night-Vision & Thermal Imagery

Night-vision devices (NVD's) magnify existing moon & star light, allowing the viewer to see in what would otherwise be total darkness. This is usually as a grainy green image. Night vision can be limited by lack of any light source, heavy rain, fog, etc. While night-vision enables the viewer to see at night or in low-light conditions, *thermal imaging* detects alterations in temperature. Thermal imaging cameras can see

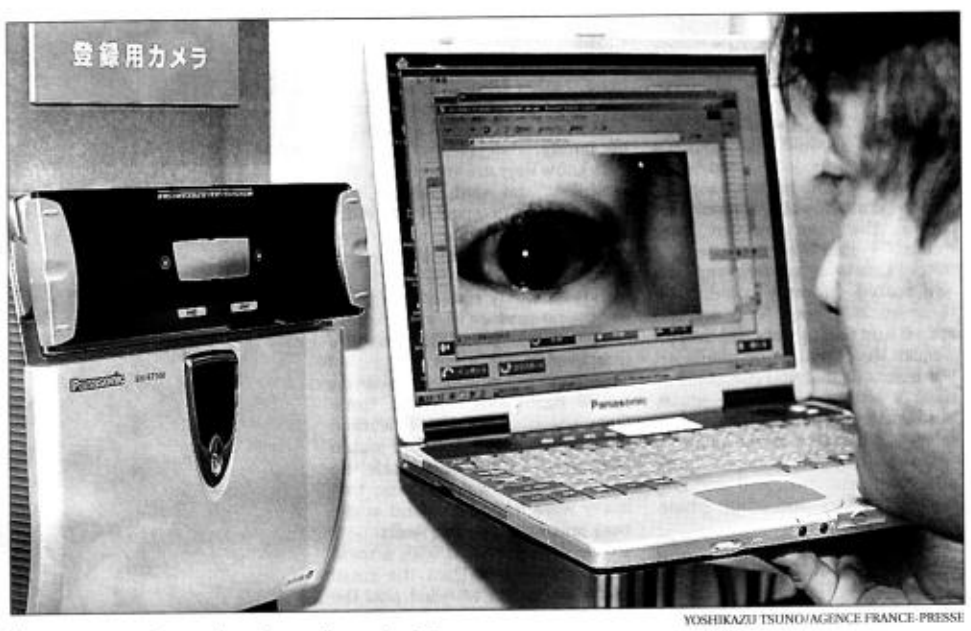
through fog and smoke, and are routinely used by fire fighters to detect the actual fire point when it is engulfed by thick smoke. Recently used vehicle engines, human forms, recently dug up earth, etc. can all be detected. Specialized thermal imaging equipment can also be used to monitor the movement of people inside a structure.


GI Joe Thermal Weapon Sight

For these reasons, both thermal imagery & night-vision are routinely used in police & military helicopters. Of the two, NVD's are far more common and are issued to regular combat soldiers and specialized police teams. Both NVD's and thermal devices can be in the form of goggles, binoculars, or rifle scopes. They are commonly used in rural surveillance where there is far less artificial light. Helicopters, planes and Unmanned Aerial Vehicles (UAV's) can be equipped with night vision and thermal imaging devices.

## Biometrics

The use of unique individual physiological traits, such as facial recognition, iris scanning, voice recognition, fingerprints, posture & walk, total body imaging, etc. Due to computer & technological advances, the use of biometrics in identifying & tracking people has become more widespread.



YOSHIKAZU TSUNO/AGENCE FRANCE-PRESSE
Iris scanning device (on left)

In terms of surveillance, biometric technologies can be used to identify persons and track them in a crowd, based on facial recognition or body imaging. Telephone calls can be analyzed to identify speakers. Fingerprints can be digitally scanned by hand-held devices to confirm or establish identities(on the spot). Many countries are now adopting biometric features for new identity cards (driver's licenses & passports), including iris scans & facial recognition. Entry into an increasing number of industrial & government facilities, office complexes, etc. now requires biometric scanning.

## Unmanned Aerial Vehicles

UAV's are commonly used by military forces for surveillance and reconnaissance. There are many types of UAV's, but all serve as aerial surveillance platforms and carry powerful video cameras equipped with night-vision & thermal. They are remotely controlled by a ground operator who observes the flight path and area through the UAV's onboard camera. Small versions, such as the Raven, Skylark or EagleScan are the size of miniature airplanes and can be hand-launched. They have a shorter flight time and are meant to be used by frontline combat troops who require a recon of a nearby area. Larger UAV's such as the Heron & Predator are the size of a small plane and can remain in flight for nearly 24 hours and fly long ranges. They can also hover at high altitudes. These larger UAV's can be equipped with missiles and have been used in targetted assassinations by Israeli and US forces.


Skylark UAV used by Canadian Forces in Afghanistan

## Satellite

Satellites are used by military, intelligence and commercial agencies for a variety of purposes, including digital imaging, communications, navigation, etc.. They are launched into specific orbits, which they then maintain during the course of their life (up to 10 years in some cases). There are hundreds of satellites in orbit around the earth.

The most advanced spy satellites are those deployed by the US, including the 'Key Hole' (KH) series of imaging satellites. The KH-12 and KH-13 versions can identity objects as small as 5" on the ground (from hundreds of miles in space). They also use radar, lasers, infrared and electromagtnetic sensors to see through cloud cover, forest canopies, and even concrete structures, to create images or gather data.

Imaging satellites are used primarily for military intelligence to monitor troop movements, weapons positions, bases, ports, cargo ships, etc. They are limited in their use for suveillance of individuals because they are in orbit and cannot hover over a specific area, and therefore cannot provide real-time video of a single location. Aerial views of tops of heads are also not very useful.

Other surveillance satellites are those used for SIGINT (signals intelligence) which monitor radio and mobile phone traffic. There are an estimated 100 US national security satellites in orbit, with 6-7 of them being imaging, and 9-11 being SIGINT. Canada and other allied states share intelligence with the US through networks such as Echelon, including data from US spy satellites.

# 7. Surveillance Detection

Confirming surveillance can often be difficult. It is usually done to determine if surveillance exists (in order to evade it). For this reason, obvious surveillance detection should be avoided. If operators think a target is engaging in counter-surveillance, they may become more sophisticated in their approach, and may believe the target is going to carry out some 'illegal' activity.

In most cases, surveillance operators will withdraw if they believe they have been detected. Surveillance itself may be stopped. In other situations, surveillance teams may maintain command of the target even if detected (overt surveillance). Obvious surveillance by police is sometimes used to intimidate targets as part of a larger psychological warfare operation, usually designed to neutralize the target through fear and paranoia.

## Detection of Physical Surveillance

The key to successful surveillance detection is **awareness** and **observation** of one's surroundings, including persons and vehicles. In identifying potential operators, make note of their clothing, size, mannerisms, and facial features (including hair style & color, shape of head & face, mustache, marks, etc.). In particular, any distinguishing marks or features can greatly assist in retention & the ability to later identify the same individual or vehicle.

Most operators will attempt to blend in and to minimize any attention being drawn to them. Colorful or odd clothing, hairstyles, etc. will be avoided due to the involuntary attention they attract. Therefore, most operators will be marked by their 'unnoticeable' and normal appearance.

In identifying possible operators, begin by observing those around you. Assume that all are potential operators. Begin eliminating those who are most likely to not be engaged in surveillance, in order to focus on those that are. Keep in mind that some surveillance teams consist of persons who look as if they could not pass a basic physical fitness test, and can include old Asian ladies, fat short men, etc. Undercover police have also infiltrated biker gangs, facilitated in part by their own personal interest in tattoos, growing their hair long, and not shaving. It is most important to evaluate what people do and their behavior, not their appearance or what they look like.

Vehicles can be observed by their color, shape, model, noticeable marks/dents, and license plates. At night, the sillhouette of the vehicle and the position of its headlights can assist in identifying possible surveillance operators.

A main goal in detection is to observe an individual and/or vehicle in one location, and then at subsequent locations.

### General Characteristics of Surveillance Operators (Foot & Vehicle):

- Can be of any race or ethnicity, any size or shape, young or old.
- They will usually avoid eye contact and can even appear awkward in their efforts to do so.
- They may appear out of place, nervous & tense (because they are).
- Can be heard or observed speaking into chest microphones, adjusting ear-pieces, or using hand-held devices to adjust volume or signal team members (contained in pocket).
- Can be observed signaling (by hand, head nod, etc.) or directly talking to other team members.

### Detection Techniques

One of the best times to detect surveillance is when a ***surveillance box*** has been established around a location. Surveillance teams are most vulnerable to detection during this phase of an operation. In some cases, they may sit for hours waiting for the target to move or appear.

**Observation Posts** in overlooking apartments or houses can often be identified by their apparent lack of activity, drawn blinds or curtains, or some other coverings over windows. Although they want to see out, they do not want you to see in. In order to see out, all they may require is a slight opening for a camera lens or telescope.

Possible OP locations can be observed from within the target location (using the method described above) as well as when leaving/entering the area. For surveillance teams, the ideal location has good line-of-sight observation of the target's front door and vehicle.

The more familiar one is with their neighborhood, the easier it is to identify new vehicles & even neighbors, both of which could be potential surveillance. Sometimes, it is impractical for police to rent out apartments or use the homes of civilians. Then, a vehicle Observation Post is used.

If a **Vehicle Observation Post** is used, it is usually a van, mini-van, camper home, or cube truck—large enough to contain operators & surveillance equipment. Like the apartment scenario, a vehicle OP will be marked by its lack of activity and by an inability to see into the rear compartment area. Curtains or some other cover are also placed on the windows. Vehicle OP's can remain parked for days or be moved around and replaced. A possible indicator of surveillance is the near-constant presence of some kind of vehicle with a rear compartment in the vicinity.

If a vehicle matching these descriptions is parked & the driver walks away, then gets into another vehicle, the parked vehicle is a potential surveillance post. In some cases, police have parked a normal passenger car with an operator hidden in the trunk. The operator can monitor a transmitter and/or video record activities through a peep hole.

A variation of the vehicle OP is the parking of a vehicle with either a device and reciever to record a nearby transmitter (in a building or on a person) or with a mini-CCTV video camera installed. The operator leaves the car for the duration of the surveillance operation then retrieves it later.

****

When leaving a location, either by foot or vehicle, the target individual discreetly observes for signs of a ***trigger*** (an operator with line of sight) as well as the *follow*—a person or vehicle which also pulls out and begins to follow behind.

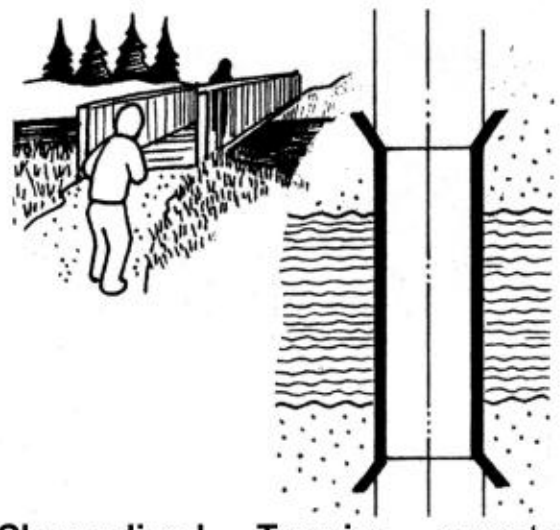
A person can also walk around the neighborhood and observe for possible surveillance. Leaving and then returning (***double-back***)-- as if something was forgotten-- can force operators to re-establish a surveillance box, potentially exposing themselves.

Another time when surveillance operators are vulnerable to detection is during the *transition* from foot to vehicle, or vice/versa. Observe for persons who rush unexpectedly to enter a vehicle, or who exit abruptly, etc.

During mobile surveillance, it is often the reactions by operators which reveal their activity. Some of this is subconscious and becomes part of the routine of surveillance operations.

For example, **mirroring** is when a surveillance operator duplicates your actions as they follow your lead, especially in vehicle surveillance. **Pacing** is when they maintain the same constant distance between themselves & the target, slowing down and speeding up to keep pace.

By taking certain routes or actions, surveillance operators can also be caught off guard.

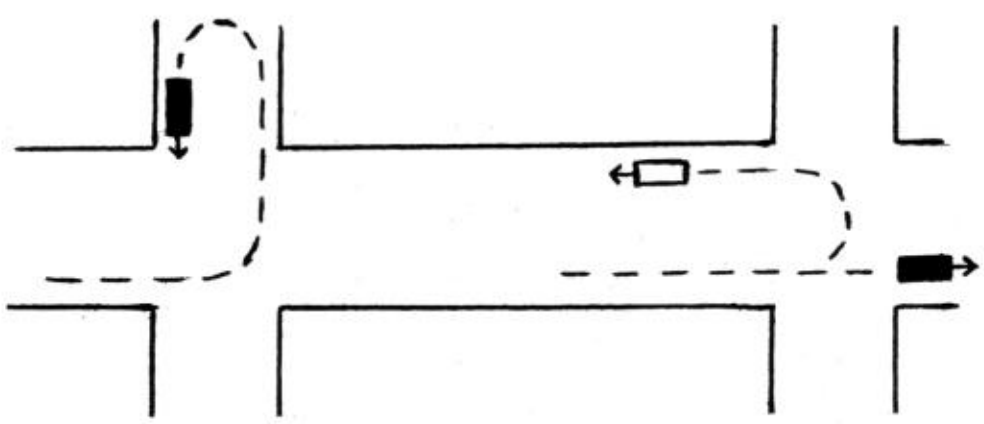


**Channelized Terrain:** operator must commit to crossing to keep command of target

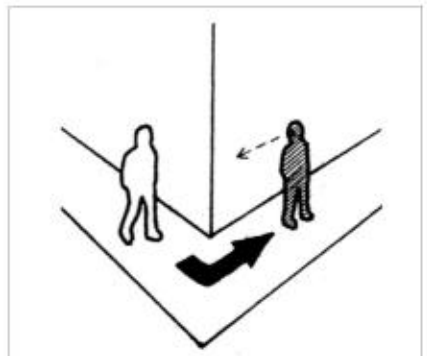
Moving through **channelized terrain** can expose surveillance operators to observation. Channelized terrain is when all traffic (foot or vehicle) must pass through a restricted passage or opening. A bridge is an example of such terrain, a tunnel, etc. In order to keep command, a surveillance team must commit to entering & crossing the terrain. On foot, a target could walk to the middle of a bridge, stop as if to enjoy the view, then turn and walk back (u-turn) to note the response of other foot traffic.

When walking or driving, sudden and abrupt **u-turns** can force a surveillance operator to respond, thereby revealing their activity. Poorly trained operators or overt surveillance will quickly u-turn as well & resume the follow. A well-trained operator will continue past and then turn off, handing command over to another vehicle/operator.

***Standard Response to a U-Turn:*** command vehicle continues straight, back-up vehicle pulls off to begin follow



When walking or driving, a **blind turn** can be used to force an unexpected response by surveillance operators. A blind turn is a sudden turn at a corner in which the target then stops and waits to observe the actions of potential surveillance operators. A standard response by surveillance will be to continue past the corner while glancing to observe the whereabouts of the target. He/she will then communicate this to other operators and pass command on to another team member. Less experienced operators may simply turn the corner also and be confronted by the target, possibly forcing an unexpected reaction.



**Blind Turn**

On foot, the only opportunity to discreetly observe to the rear is when crossing an intersection. Sudden crossings in the middle of the street (**jaywalk**) also allow for rear views and may catch operators off guard. Entering **public locations**, such as malls, office complexes, etc., can force surveillance to enter with you and expose themselves to closer observation. Going up or down a series of escalators allows for logical 180-degree turns to observe to the rear. Elevators could force operators into even closer proximity. Multiple levels also enable a target to observe large areas from a dominant & overlooking position.

**Public transit** can also be used for detection purposes. Getting on buses or subways can force operators to get into close proximity with the target or risk losing command. When operators must get on transit with a target, this provides good exposure of facial features and can force unnatural responses from operators. Observe those who arrive at bus stop after you and board the same bus, as well as those already on the bus and seated to the rear, and those who board at subsequent stops. Foot operators may also be dropped off after the target gets off, therefore if the same vehicle is seen near bus stops en route, or even following the bus, this is a possible indicator of surveillance.

On **highways**, pulling off onto the shoulder prior to a rest area may force surveillance vehicles to pull off and wait. Driving through the rest area, a target can observe which vehicles are there and then identify them at subsequent locations. Like subways, highways are characterized by high speeds which can catch surveillance operators off-guard. Exit ramps, turn offs, rest areas, u-turns, blind-turns, etc. can all be exploited on highways. Highways also offer observation over longer ranges and for extended periods of time.

In both foot & vehicle surveillance, command may be shifted frequently to minimize exposure of operators. Often, unpredictable or sudden moves can force surveillance teams to react. However, if your pattern up this point has been routine & predictable, operators will become suspicious. Detection of surveillance is best done as covertly as possible. In a vehicle, use rear-view mirrors. Wrap-around sun glasses can also aid in discreet observation by shielding the eyes.

**Rural:** From one's location, potential OP's can be identified. They must have line-of-sight observation. The only way to find possible OP's is to physically walk the area. OP

sites can be identified by flattened out or disturbed areas used for sitting or sleeping, as well as tracks, litter, equipment dropped by operators, etc. Knowledge of tracking can greatly assist in identifying potential OP sites. Longer term OP's may consist of a hide left in place. Detection can be greatly assisted by dogs, as well as observing the responses of animals & birds (in many police raids, dogs have been the first to be shot).

## Detection of Technical Surveillance

Technical surveillance is difficult to detect, especially that involving telecommunications. A general rule in regards to technical surveillance is to assume it is always possible and to protect information as if it were subject to eavesdropping. Even using technical counter-measures to detect surveillance devices or technologies is not a guarantee of security. Our enemy has far greater technological resources, including access to telecommunications facilities, corporations, etc. This determines our means of security against technical surveillance.

One purpose of physical surveillance is to enable police-intelligence agents to plan physical break-and-enters in order to put in place technical devices. Special entry teams may first break into a residence, workplace, or vehicle and photograph interior walls, fixtures, layout, objects, etc. They determine the best locations and types of devices to be used. They then leave, prepare the devices, and return.

In many cases, there is no obvious sign of entry and nothing is taken. If dogs are inside the house, they may act strange due to ultra-sonic devices used to control them during police covert entry. In other cases, burglaries may be staged. Telephone, TV, electrical repair crews or plumbers may be used to gain access. A co-operative landlord might provide keys. Police raids & searches are also good times for devices to be put in place.

Items seized by police during a raid, such as computers, VCRs, etc., and later returned, could have devices planted in them. The same is true for vehicles impounded over night or unexpected gifts such as steros or TV's (trojan horse).

A possible indicator of electronic surveillance (bugs or cameras transmitting) are irregularities in radio, TV or cell phone connections.

Before digital technology, phone tapping was clumsy and often resulted in clicking sounds, lower volumes, etc. Today, phone tapping can be done more effeciently with no tell-tale noises.

**Searches for technical devices** should be conducted as discreetly as possible, carried out while pretending to clean up, etc. In some cases, suspects have been raided shortly after finding listening devices in their residences & vehicles. Searches should be systematic and planned, from the ceiling to the floor, including all objects, devices, light switches, electrical outlets, light fixtures, air vents, smoke detectors, etc. in each room. On wall surfaces, small off-colour pieces, differences in texture, or pin-holes, may be detected. Using a small flashlight to focus on small areas helps in observation. All electrical items should be dismantled & inspected, all paintings & mirrors removed. Drapes & curtains should be checked, as well as plants, furniture, desks, etc.

Listening devices or mini-cameras can also enter a location as a 'trojan horse', concealed in gifts such as new clocks, radios, CD players, small TV's, etc.

**Vehicle searches** should be carried out after a car-wash. Park vehicle in discreet location (i.e., garage) and inspect undercarriage for tracking devices attached by magnet. Check inside the trunk and engine. Check the interior, including roof, door paneling, dash board, visors, and seats for devices.

Listening devices which rely on radio frequencies can also be detected by RF monitors. If radios, TV, or phones begin picking up different frequencies, static, or behaving strangely, this is a possible indicator of surveillance.

If technical devices are found, this is a clear confirmation of surveillance. What is done with this information depends on the situation. Devices can be left in place, as removing them can prompt a police raid to retrieve them, and/or more sophisticated devices to replace them. Misinformation can be provided. At the last moment, tracking devices can be re-attached to another vehicle, etc.

## Security Against Technical Surveillance

In enclosed spaces such as rooms & vehicles known to police-intelligence agents, or on any telecommunicaitons, it is almost impossible to secure against technical surveillance. When protected information or activities must be discussed, **avoid all enclosed spaces** associated with oneself or movement members, and **avoid using telecommunications.** The best form of communication is face-to-face.

The rule is: ***against a high-tech enemy, go low-tech (or no-tech)***. Do not attempt to overcome technical surveillance using technical means.

### Telecommunications

Assume all telecommunications are vulnerable to surveillance and avoid discussing protected information or activities on the phone, internet, etc. Since counter-insurgency operations are based on all sources, avoid discussing personal information on the phone or internet, including rumours, gossip, and private details of individual's lives. Use pre-arranged code words and names if it is necessary to communicate over telecommunications.

### Cell Phones

Cell phones can be used as both tracking & listening devices and should not be carried during any secret activity or when discussing sensitive matters. The battery should be removed.

### Computers and Internet

The following are basic tips from *A Practical Security Handbook for Activists & Campaign,* a publication from resistance in the UK (www.ActivistSecurity.og). Overall, however, all telecommunications should be considered insecure forms of communicating.

**Computer Security**

**1.** Install and regularly update anti-virus and firewall software. Free programmes such as AVG (www.grisoft.com) and ZoneAlarm (www.zonealarm.com) are available for Windows. The important feature is that live update is activated so they are continually up-to-date.

**2.** Install a spyware detector programme such as Ad-Aware which is free from www.lavasoft.de.

**3.** Deleting a file does not remove it from your hard drive, etc. In order to do this it needs to be properly wiped, using a programme dedicated to doing this. Recommended ones are Clean Disk Security and PGP.

**4.** Encrypt any sensitive files on your computer, CDs or floppy disks using a programme such as PGP (or GPG). Ideally, you will stuff all files in to one big archive (eg using WinZip or StuffIt) and encrypt that. This means that even the file names are hidden. Wipe the original files. This should be done every night when you've finished using the computer. Alternatively use disk encryption

**5.** Chose passwords that are effective – longer than 16 characters, including upper and lower case letters, number and symbols if permitted. Weak passwords are easily broken. Password protected computers are not secure to the prepared infiltrator so encrypting anything sensitive is also needed.

- Passwords should be changed on a regular basis.
- Do not write them down and stick them under your chair or desk – these are the first places that a spy will look.
- Do not base them on the names of family, pets or dates of birth
- Do not simply use dictionary words

**6.** Back up your computer in case it is stolen but keep the back-ups secure somewhere else.

**7.** Consider switching away from Windows to other operation systems such as Linux or Mac.

**8.** Avoid wireless keyboards as they transmit quite a distance as well as to your computer.

**9.** Keep important/sensitve data and PGP keys on removable media such as memory sticks[USB drives].

**Internet Privacy**

**1.** Emails are not secure, and very easy to monitor. To keep them private, use PGP encryption (www.pgpi.com). Don't say anything in an email you would not be prepared to justify in court.

If you want to contact another person without those watching you knowing who it is you are in contact with set up fake email accounts... and use them instead. Consider using it as a maildrop system [do not send emails, save them as drafts—you communicate with others through the draft emails left].

**2.** Be aware of spam – unsolicited emails, even if they look genuine, such as from a bank. Never buy anything, or even click on the links to websites contained in unsolicited emails...

**3.** Every time you access the internet you leave a trace that can be used to tie back to you. If visiting a website you don't want people to know you are interested in, use an anonymizer website or an internet café. If you suspect you are being monitored, do not do anything sensitive from your home computer. Watch out for CCTV in internet cafes so pick small, obscure ones [or use disguise].

**Listening Devices/Mini-Cameras**

To protect against covert entry & placement of devices in a residence or vehicle, standard anti-burglar measures are used. These include good, strong locks on doors & windows, alarms, surveillance cameras, and dogs. Vehicles can be parked in secure garages with an alarm system. None of these measures will guarantee security against covert entry, however.

Biker gangs began using scanners in their residences and clubhouses to detect transmitters hidden on infiltrators or informants. In response, police created recording devices concealed as pagers with on/off switches so that if a scanner was known to be in use the device could be turned off.

Bikers would also buy and set up CCTV camera systems in their residences, drug labs, and clubhouses, to monitor them for covert or forced entries. Hidden voice-activated recorders were also used in efforts to identify covert entries.

To disrupt police surveillance, biker gangs would position sentries and have patrols for a four-block radius around a meeting point (i.e., a clubhouse). This forced undercover operators to pull back and find safe areas from which they could receive transmissions. Another technique was to meet in one location (a rendezvous point) and then go to another, known only to a select few, that offered good counter-surveillance terrain. In one case, the bikers met in a rural area near an airport, limiting the use of an aircraft used as a back up reciever.

To counter listening devices, bikers began using dry-erase or chalk-boards to write down secret information, then erasing it. Writing notes on single pieces of paper against a hard surface (to avoid impressions) then destroying them after reading is a variation of this technique.

To avoid listening devices (inc. parabolic mics), conduct secret talks while walking in secluded areas or in impromptu locations.

Use pre-arranged code words and names to avoid referring to actual information.

*Code:* letter-number key. Choose a ten letter word in which no letter is repeated and assign a number to each letter:

J A M E S  B R O W N
1 2 3 4 5  6 7  8 9 0

*Example:* WRE-WBNA = 974-9602
Code on phone: the black singer

**Tracking Devices**

WorldTracker GPS tracker, commercially available

To counter the use of tracking devices, do not use personal vehicles for secret activities. Newer model cars also have built-in GPS trackers, such as On-Star. Many rental car companies now install GPS devices to track their vehicles. It is also possible that police could place a GPS tracker on a bicycle. Any vehicle used to counter surveillance must be 'cold'-- unattached to you or any comrades.

### Aerial Surveillance & Night Vision

To evade aerial surveillance go inside malls, apartment buildings, transit stations, or any building that has multiple exits and large crowds. Change jacket and hat if possible.

To evade night time aerial surveillance (i.e., night vision/thermal) in an urban or suburban area, go into large buildings, under concrete bridges, under vehicles, into sewage or tunnel systems, etc.

In rural areas go under bridges, drainage pipes, underwater, under rocky overcrops, thick forest, tunnels, etc. to evade aerial vehicles at night.

One danger in hiding in a fixed position is if you're already being tracked by aerial surveillance they will see this and direct ground units to your location. You may not be aware you are being observed due to aerial surveillance being conducted at an altitude beyond your hearing range.

Some measures reportedly used to counter infra-red and thermal imagery include the use of 'survival blankets', a sheet of foil that traps body heat (and reduces thermal signature) and water immersion (which also reduces thermal signature).

## 8. Surveillance & Evasion

Anti-surveillance actions are usually taken in order to evade police-intelligence while carrying out secret activities. When preparing for anti-surveillance, a targeted individual should consider their patterns of movement & activities over the previous time period. This identifies possible times, locations, or methods by which to evade surveillance. After a long time doing surveillance, operators may themselves fall victim to this routine and become vulnerable to anti-surveillance actions.

The main goal of anti-surveillance is to evade police-intelligence agents. If able to escape the initial stakeout or surveillance box, for example, the target then defeats surveillance and can move without threat of being observed. Techniques used to detect surveillance, such as u-turns, double-backs, blind corners, etc., can also be used & built upon in order to evade surveillance.

Evading stakeouts or surveillance boxes can be done from any location and need not begin with one's residence. Public locations with multiple & even hidden exits can be used. Public transit can be utilized to break up surveillance teams en route to a suitable public location, etc.

**Disguises** can greatly enhance anti-surveillance actions. Operators must recognize the target in order to follow him/her. Although facial features are the best way to identify specific individuals, operators also rely on form, dress, and mannerisms. One's physical appearance can be altered in a number of ways:

- Baggy or loose-fitting clothing can alter form. Filling them out can make a person look larger & bulkier.
- Changing clothing style & colors.
- Changing one's posture & pace.
- Use of wigs and theatre make-up.

If the use of disguise is detected, surveillance operators will assume the target is intent on evading their efforts and is preparing to carry out some protected activity. Great care & planning should be put into any anti-surveillance action, and disguises must be effective. Consideration should also be given to changing shoes.

In an urban environment, anti-surveillance actions carried out on foot have more likelihood of success than those done by vehicle. There are a limited number of areas a vehicle can travel (streets, highways, alleys, garages, etc.). In addition, they could have tracking devices attached, so no matter how many turns & u-turns are used, operators still know where the vehicle is.

In contrast, foot travel is almost limitless. Targets moving on foot can exploit terrain & routes of travel to break up or elude surveillance teams. Public transit, especially subways, are difficult for operators to follow on, due to the high-speeds, ability to change directions, multiple exits from stations, etc. Public location such as malls, office complexes, etc., are also difficult due to multiple exits, different floor levels, elevators, escalators, etc. In an emergency (i.e., a fire alarm) operators would have even more difficulty following a target.

Evading surveillance is best done at night or in bad weather (i.e., a rain-storm,), in order to limit visibility.

In an urban setting, and in public locations, it is often the most illogical moves which can identify surveillance operators or limit their ability to follow (which may also alert operators that you are carrying out some kind of anti-surveillance actions). Taking an elevator one floor and then walking back down is illogical, and any one else doing so would be highly suspicious. Waiting at transit stops as buses or subway trains pass by can force operators to board at least one of these, or risk exposure. Taking a bus or train to the end of the line and then returning can also identify potential operators. Getting on & off transit repeatedly can further break up a surveillance team.

## 9. Informants & Infiltrators

Informants and infiltrators are spies who gather information on the resistance & provide it to the enemy. They may also take a more active role. These acts can result in capture, arrests, imprisonment, and death. The term collaborator is used for any member or citizen who aids or assists our enemy.

Informants & infiltrators provide unique & special *human intelligence* (i.e., emotional states, plans, intentions, etc.) which can be gained in no other way. In addition, infiltrators & collaborators can physically disrupt & sabotage movement activities. They can spread disinformation & poisonous gossip, creating division and paranoia. They can also record incriminating statements and actions. Overall, they are an essential & active element in counter-insurgency operations as well as criminal investigations.

**Informants** are persons recruited by the state security forces to provide information. They are civilians, usually friends or associates of the target group. They could be embittered comrades who feel isolated or even betrayed by the group. Or, they could be genuine members arrested and subject to pressure. Police refer to them as 'Confidential Informants' or 'Confidential Sources'.

***A standard method of recruiting informants is to find people (in or near the group) with problems.*** Persons most vulnerable to becoming informants are those seeking protection, those seeking revenge, drug addicts, alcoholics, those suffering from trauma or mental illness, those facing long prison sentences, & those in compromised situations (blackmail). Intimidation & coercion may also be used to make a person become an informant. Money can also be a motivating factor in making a person turn informant, and in maintaining their services over an extended period of time.

Potential informants may also be identified through surveillance. Personal relationships, drug or money problems, sexual activities, personality conflicts, internal power struggles, etc., are all analyzed in order to find an opening through which to exert pressure on a potential informant.

Movement members who are arrested & subject to pressure may break down and collaborate with police. In some cases, this may result from a lack of faith in the struggle. It is important that members are not pressured, coerced, or intimidated, into carrying out activity, but that they do so out of a strong belief in its necessity. Studies have found that those most resistant to torture are motivated by ideology, not economic self-interest or social prestige, for example.

Once a person is turned informant, they are increasingly dependent on their police-intelligence 'handlers' for protection, having betrayed their former friends & comrades. Informants may be low-key members or associates who quietly gather information & observe, while others may be encouraged to become more active by their handlers, acting as an *agents provocateur* (an informant or agent who provokes actions, usually illegal and which lead to arrests).

**Infiltrators** are civilians recruited by the state security forces (or corporations), or police-intelligence agents. They insert themselves into the group by posing as genuine members of the resistance, to greater or lesser extents. They can be of any race or ethnicity, size or shape, etc.(depending on the target group of course). Police infiltrators have proven on occasion to be very adept at playing their role, looking and acting the part (i.e., undercover investigations of biker gangs).

Infiltrators can be long-term & deeply imbedded in a group, forming intimate friendships, having a general intelligence gathering role or as part of a criminal investigation. Or they can be temporary operatives perhaps with a specific goal (i.e., to neutralize key leaders or groups). Some infiltrators are also referred to as *agents provocateurs* for their leading role in instigating (often illegal) activities.

Infiltrators are usually developed over a period of time, during which they meet & establish rapport (a friendly relation) with members of the target group. This could begin with chance encounters, shared interests, meetings, events, rallies, etc. All these, of course, are the result of extensive surveillance and psychological profiling (they know when & where to be, and how to act). One common method is for an informant to introduce the infiltrator to the group. Infiltrators might befriend one member in order to gain contact with the entire group.

Infiltrators can also enter a group as genuine members from another area or region, where they first made contact with the movement. They can claim to know certain people, or to have been at certain places & events, in an effort to establish credibility. A common cover used for radical groups is that of a student; in fact, universities are recruiting grounds for intelligence agencies in general.

In some cases, infiltrators provide resources, including money, vehicles, weapons, or information—things which are of great value & which raise their profile & influence in the group. They may also attach themselves to key leaders or assume leadership and security positions in order to extend their influence & access to information (see below, FBI COINTEL-PRO Techniques).

Notes from *Security Culture: A Handbook for Activists,* Nov 2001 edition:

## Types of Informants

- The "hang around" type: they are persons who regularly show at meetings and actions but generally don't get involved. They collect documents, listen to conversations and note who's who. This observation role is relatively inactive.

- The "sleeper" type: is similar to the "hang around" modus operandi, except that their absorption of information is used to activate their role at a later date.

- The "novice" type: presents a somewhat more active role, but confines themselves to less prominent work. They don't take initiative, but the work they do is valued. This helps them build trust and credibility.

- The "super activist" type: they come out of nowhere and all of a sudden, they are everywhere. Whether it's a meeting, protest, or an action, this person will be right in the thick of it. Keep in mind however that this can also be the mark of a new activist, whose enthusiasm and commitment is so strong that she/he wants to fight the power every minute of the day.

"It should be said that with several of these *modus operandi,* the behaviour is hard to distinguish from a sincere new person's involvement. How do we tell them apart? Well, a planted infiltrator will ask a lot of questions about the direct action groups, individuals and illegal activities. She/he may suggest targets and volunteer to do reconnaissance as well as take part

in the action. Infiltrators also try to build profiles on individuals, their beliefs, habits, friends, and weaknesses. At the same time, infiltrators will shield their true selves from other activists.

"Anyone who asks a lot of questions about direct actions isn't necessarily an infiltrator, but they ARE someone you should be careful with. At the very least, they need to be informed about security issues. New activists should understand that direct action tactics can be risky (though some risks are worth taking!) and that asking a lot of questions endangers people. If the person persists in asking questions, there is a problem and appropriate measures must be taken. Activists who can't understand the need for security should be kept away from situations in which they might incriminate others."

## The Undercover Infiltrator

"A deep cover agent is equipped with false ID (usually retaining the real first name so he/she doesn't forget to respond to their name), and a skeleton of personal history, such as a business owner who will verify that so-and-so worked for them (and who will later notify the police that someone was inquiring). The agent's background may be kept close to the truth to prevent slip-ups. Finally a deep cover agent may work a real job, rent a house or apartment, and live the role 24 hours a day.

"An undercover cop working under "light" cover may also have a false ID, but will most likely go home to his family and "real" life (usually in another city). Sometimes narcotics officers and other specially trained agents will be called on for these assignments."

(*Ecodefense: A Field Guide to Monkeywrenching,* Foreman and Haywood, Abzzug Press,Chico CA 1996, p. 296).

## Informant-Handler Meetings

As part of an undercover operation, the infiltrator/informant must exchange information, equipment or money with their 'handlers'. The most secure method is face-to-face meetings. The FBI, for example, has rented apartments for informant and handler to meet at, as a 'dead-drop' to leave messages, recordings, etc., and as a safe house to sleep at. At other times the informant and handler would meet in parking lots, one getting into the other's car:

"To maintain security, Tait [an informant in the Hells Angels] and the agents met in secret places... An agent would stop in an indoor parking lot and Tait would hop into his car. They would drive to another city to talk in a motel or public place while two other agents carried out counter-surveillance." (*Hells Angels: Into the Abyss,* by Yves Lavigne, HarperCollins Publishers Ltd., Toronto 1996, pp. 237-38)

When they had to communicate over telephone, one would phone the other's pager and leave a phone number they could be reached at. Even then, their conversations were limited and coded:

"Tait paged McKinley [FBI handler] in Oakland to break the news. He never called McKinley's house because the Hells Angels had access to telephone company records... Likewise, McKinely always paged Tait." (*Hells Angels: Into the Abyss*, p. 147)

# Dealing with Informants & Infiltrators

Like surveillance, detecting informants & infiltrators can be difficult. Some work very hard to conceal their activities and to play the role of a genuine member of the movement. Intuition, observation, and analysis of a person's activities & conduct can help identify possible informants & infiltrators. Background checks should be carried out on suspicious persons to confirm their identity (although a well organized operation will have 'backstopped' any infiltrator's fake ID). Group's can also organize their own surveillance operations to learn more about suspicious persons.

Unless there is strong evidence, public accusations & denouncements can sometimes cause more damage than good. They may appear as overly paranoid, personal attacks/rivalry, etc., especially if there is no hard evidence. In many cases, suspected infiltrators can be discreetly prevented from involvement in critical activities (i.e., communications, funds, transportation, discussions on tactics & strategy, etc.).

When infiltrators and informants have been confronted, their most common reaction is to deny the charge outright. They often emphasize all the risks, sacrafices, and loyalty they've displayed. They use emotional responses to gain sympathy from other group members (who may be unaware or unconvinced the person is an informant or infiltrator).

If a person is identified as an infiltrator or informant (i.e., as a result of court disclosure, finding notes or recording devices, or through admission), photos should be taken of them in order to inform others. A video taped statement should be obtained if possible. Any materials or areas a confirmed informant or infiltrator has had access to should be assessed for risks, security codes changed, etc.

## Background Checks

"What are some ways of looking into the possibility that someone is an informer? Firstly, unless you have concrete reasons or evidence that someone is an infiltrator, spreading rumours will damage the movement. Rumours that you do hear of should be questioned and traced back. A person's background can be looked into, especially activism they claimed to have participated in, in other places. Do your contacts in those places know of the person, their involvement? Did problems ever come up? One important advantage of having links with far away places is that it makes it more difficult for informers to fabricate claims about their activities.

"What are a person's means of living? Who are her or his friends? What sorts of contradictions exist between their professed ideals and how they live?" (from *Security Culture: A Handbook for Activists*)

In one ATF undercover operation against the Hells Angels (Operation Black Biscuit), the agents were so well 'backstopped' with fake ID and histories that the biker's counter-intelligence, which involved extensive background checks, failed to uncover their true identity. Private investigators hired by the bikers, along with other intelligence sources, only re-affirmed the fake ID's of the agents, and provided a false sense of security to the gang.

# 10. FBI COINTEL-PRO:

## Domestic Counter-Insurgency Campaign (1960s-70s)

The FBI's infamous Counter-Intelligence Program (COINTEL-PRO) should serve as a chilling reminder of the length to which our enemy will go to crush our resistance. This is especially true since veterans of this time are still with us, & many remain in prison to this day as a result (inc. Leonard Peltier, Mumia Abu-Jamal, etc.). Many are also dead, killed by the FBI, police, & paramilitaries during the 1960's & 70's. Our failure to learn from this time would not only leave us vulnerable to the same tactics, it would be a dishonor to the sacrifices made by the previous generation.

COINTEL-PRO had its roots in the anti-communist campaign of the 1950s (when the Cold War began). Its first targets were communist & socialist groups, as well as the black civil rights movement. In the 1960s, new liberation movements emerged around the world. US involvement in Vietnam & the fierce resistance of the Vietnamese people contributed to a climate of insurgency & rebellion, one that extended into the US itself.

At this time, COINTEL-PRO was expanded nation-wide, involving extensive surveillance, informants, collaborators, assaults, false charges, imprisonment, fabricated communications, smear & disinformation campaigns, burglary, vandalism, arson, as well as lethal force. Many key organizers were assassinated, and many are still imprisoned. Among the hardest hit were the Black Panthers & the American Indian Movement, although the Chicano, Puerto Rican, and anti-war movements were also targeted.

The goal of this counter-insurgency campaign was to destroy organized resistance movements, using any means necessary. A major focus was instilling a sense of ***paranoia*** & ***fear*** among movements, in order to neutralize them. Those who refused to submit were targeted with harsher methods, and some killed. Violent assaults & deaths contributed to over-greater paranoia & insecurity. By exploiting internal divisions during a time of intense repression, the FBI/police were successful in neutralizing this first phase of current resistance in North America (but they couldn't kill the spirit).

COINTEL-PRO was exposed after unknown persons broke into the FBI's Media, Pennsylvania offices in 1971. Government hearings and inquiries gave the impression that COINTEL-PRO ended; however, domestic repression continued throughout the 1970s, '80s, and '90s. Today, new anti-terrorist laws such as the PATRIOT ACT have legitimized much of what occurred under COINTEL-PRO and have even extended the powers of FBI, police & intelligence agencies.

In Canada, the RCMP have been one of the best students of the FBI, serving as a similar national police force with a role as a 'political police' as well as an early force of colonialism. In the 1970s the RCMP were exposed for carrying out illegal activities against dissident groups including burglaries, vandalism, theft, and arson. During the 1995 siege at Ts'Peten (Gustafsen Lake, BC) the RCMP fabricated shooting incidents & used lethal force in agreed-upon 'no shoot' zones. An RCMP media relations officer was caught on video saying: 'Smear campaigns are our specialty'.


## COINTEL-PRO Techniques:

### 1. Surveillance

Extensive & wide-spread surveillance was used to gather information on groups & individuals, both technical (bugs, wiretaps, telephone, mail, photo & film) & physical (personal & vehicle). This info often formed the basis for further COINTEL-PRO operations. FBI & local police agencies, along with other law enforcement agencies, were involved. Surveillance itself was often used as a means to induce paranoia & fear (by surveillance being obvious & belligerent).

### 2. Infiltrators, informants & collaborators

Widespread use of infiltrators & informants was a key part of the FBI's COINTEL-PRO. Informants, usually disaffected members or associates of a group, were recruited through intimidation and/or money. They provided critical human intelligence. In the case of infiltrators & collaborators, they also actively disrupted organizations & enabled FBI/police to carry out deadly assaults, frame-ups, etc.

Infiltrators included FBI agents, undercover police, and civilians. In some police departments, 'red squads' worked with anti-gang units to prevent unity between gangs & resistance movements. They also recruited infiltrators from gang members facing jail or for money.

Infiltrators were often able to provide information & resources (via their FBI/police handlers) to the group. Because of their experience with weapons & violence, they were often promoted to high-ranking positions in the organization, with some being in charge of security for chapters or leaders.

How did the movements become so heavily infiltrated? They were completely open & public organizations, which actively recruited members from the general public. Infiltrators were easy to place. The only area in which security measures were taken was at the leadership level, and this is where some of the greatest mistakes were made.

In both the Black Panthers & AIM, infiltrators gained access to this inner circle, frequently in charge of security for the group itself. Some played the role of an 'ultra-militant', promoting violence & attempting to draw the group into carrying out illegal actions. Criminals/hustlers turned infiltrators were also sources of drugs, weapons, & anti-social violence within groups. Other activities included planting evidence, stealing funds, sabotage of equipment or organizing efforts, supplying information leading to arrests or deaths, as well as spreading disinformation, paranoia, & division.

### 3. Bad-jacket, or snitch-jacket

When a genuine movement member is portrayed as being an informant (or a thief, a rapist, etc.). Often, other informants are used to spread rumours, plant evidence, etc. In their efforts to attach a bad-jacket, police may frequently arrest a target during raids, but then quickly let him/her go (while others remain in jail). Police themselves may gossip or leave evidence indicating a person is an informant.

The purpose of the bad-jacket is to neutralize the target individual as an effective organizer. This technique resulted in interrogations, assaults, and even executions of suspected informants (as occurred among the Black Panthers).

### 4. False communications

Fake letters were sent between individuals or groups with misinformation (i.e., allegations of sexual affairs between members, death threats, etc.). When hostilities existed between groups, this was exploited to the point where assaults & even deaths occurred.

Another example of false communications was the production of fake newsletters, posters, etc. by the FBI/police, and distributed as genuine movement publications. This technique was effective in cutting funding for one Panther chapter's breakfast program after offensive comics were sent to funders.

### 5. Media disinformation

In collaboration with corporate media, the FBI & police would conduct 'smear & disinformation' campaigns against movements, organizations, & individuals, portraying them as violent, criminal, terrorist, or insane.

### 6. Arrests/false evidence/frame-ups

Petty charges & outright frame-ups were used to tie peop le & groups up in the court system, and to imprison many with harsh sentences. Constant or massive arrests & charges drained movements of time & resources, diverting them from resistance to legal defense. Imprisonment served to neutralize organizers while scaring away the less-committed. Scores of political prisoners & POWs remain in US prisons to this day, imprisoned in the 1970s as a result of COINTEL-PRO. Arrests & imprisonment also served to criminalize movements & groups.

### 7. Other harassment

Other forms of harassment used by the FBI & police included approaching members at their homes or workplaces for interviews, approaching landlords, employers or family members to exert pressure on members (i.e., having them evicted, losing their jobs, or facing ostracism by family). Agents would also cancel bus reservations on behalf of an organizing group, or announce that meetings, rallies, etc. had been cancelled.

### 8. Burglary, Vandalism, and Arson

FBI and local police routinely broke into offices and homes in order to steal files, copy them, and/or to destroy equipment. Offices were also set on fire, destroying valuable resources such as printing presses, files, archives, etc.

### 9. Pseudo-Gangs

False groups set up by police-intelligence agents to discredit the movement & entrap genuine movement members. In the 1960s & '70s, the FBI set up many pseudo-gangs to disrupt campaigns (i.e., among Puerto Rican *independistas*, anti-war groups, etc.).

### 10. Lethal force

Key organizers were killed by police during raids & assaults, by vigilantes (including right-wing racists), by FBI-police infiltrators, or as a result of 'bad-jacketing'. Scores were killed during the 1950s, '60s and '70s, including:

- Fred Hampton & Mark Clark (Black Panthers) were both killed during a police raid on their Chicago home, in 1969.
- Alprentice Carter & Jon Huggins (Black Panthers) were killed in 1969 by members of a rival group in a COINTEL-PRO instigated feud.
- George Jackson, a prisoner & a prominent Black Panther, was killed during an alleged escape attempt in 1971.
- Fred Bennett, an SF Black Panther, was executed by comrades after being successfully 'bad-jacketed' by an FBI infiltrator, in 1969. One of the Panthers involved in this, Jimmie Carr, was himself 'bad-jacketed' and executed by other Panthers in 1972 (!).

### 11. Assisting Paramilitary Death Squads

On the Pine Ridge reservation in S. Dakota, at least 67 members or associates of AIM were killed by BIA police, FBI, and paramilitary forces (the Guardians Of the Oglala Nation, GOONs, as they referred to themselves) from 1973-76. The GOONs, employed by a corrupt tribal president, were armed, equipped, and supported by the FBI as part of its counter-insurgency effort against Indigenous resistance. They carried out a reign of terror against AIM & traditionalists on the reserve, including fire-bombings, assaults, drive-by shootings, and killings.

Other examples of the use of paramilitary & vigilante groups include the FBI's assistance to right-wing groups such as the Minutemen, Secret Army Organization, and the Ku Klux Klan. These and other groups were provided information, equipment and weapons to carry out assaults and lethal attacks. Some were also linked to US military intelligence units. Paramilitary death squads are common in the global south.

## Assassination of Fred Hampton & Mark Clark 1969

Fred Hampton & Mark Clark were members of the Chicago chapter of the Black Panther Party. Hampton was a young & promising leader, a highly effective organizer who had begun forming alliances with other movements and even street gangs in Chicago, including the Blackstone Rangers.

In 1968, FBI infiltrator William O'Neal joined the chapter. O'Neal was a petty criminal, charged with car theft and impersonating an FBI agent using false ID. In exchange for dropping these charges, O'Neal agreed to infiltrate the Chicago chapter. He quickly became head of security and Hampton's bodyguard. This was based on his experience with weapons & violence.

William O'Neal,
FBI gangsta Infiltrator

In order to stop the Panther/Blackstone Ranger alliance, fake letters were sent to both groups with warning & threats about one or the other. This later resulted in violent conflicts between the groups, instigated by O'Neal.

O'Neal constantly agitated for armed attacks & robberies, offering training & weapons (the 'ultra-militant'). He recommended getting a plane to bomb city hall, that all Panthers be armed, and that an electric chair be installed in order to interrogate/torture suspected informants (all refused). He himself brought in firearms used as a pretext for a police raid in June 1969 of the Panther offices. Such raids were again carried out in July & October of that year.

O'Neal, along with other infiltrators, also stole Panther financial records, files, books, tapes, films, etc. in order to sabotage their efforts. The FBI also manufactured fake comics, which were sent to funders of the Breakfast Program. The comics were so offensive that many funders withdrew their support.

In November 1969, the FBI and local police began planning the assassination of Hampton. O'Neal supplied a detailed floor-plan of Hampton's apartment, including his bed and the location of his head while sleeping.

On December 4/69, fourteen heavily armed police raided the apartment using a warrant to search for "illegal weapons." Earlier that night, O'Neal had made a dinner for the residents, including Kool-Aid spiked with a sleeping agent. At around 4:30 AM, police kicked in the door and immediately shot Mark Clark, who was seated in the front room and armed with a shotgun (security against just such a raid). Unfortunately, Clark was passed out due to O'Neal's Kool-Aid.

Police then directed their gunfire against the wall where Hampton's bed was and in the area of his head. Both Hampton and Clark were killed, while others were wounded. Chicago police claimed it was a 'wild shootout' with heavily armed Panthers, although the only shot fired by the Panthers was when Clark's shotgun went off in reflex to his being shot by police. (O'Neial reportedly killed himself in the 1980's)

## Douglas Durham, 1973-75

Douglas Durham was a non-Native infiltrator into the American Indian Movement, working for the FBI. He was a former Iowa police officer who had also worked for the CIA and who had some Special Forces military experience. He was trained in demolitions, sabotage, burglary, etc.

In the early 1960s he was involved with organized crime, including a prostitution ring. This activity led to conflicts with his wife, who died as a result of a violent assault by Durham in July 1964. He was fired from the police and found to be a violent schizoid "unfit for public service."

Durham again began working as a police intelligence agent in 1971. He was present during the siege at Wounded Knee 1973, posing as a reporter. He then joined the Iowa chapter of AIM, dyeing his hair black and wearing brown contact lenses. He claimed to be a quarter Chippewa.

Based on his background & skills, Durham became head of security for national AIM and a body guard to Dennis Banks, one of AIM's national leaders. During the Wounded Knee trials of 1974-75, Durham oversaw all legal discussions & strategies, as well as taking control of much of AIM's overall administration through its national office in Minneapolis (including funds).

Like other infiltrators, Durham advocated outrageous schemes including kidnapping politicians, armed confrontations, etc. He is suspected in the death of at least one person—Jancita Eagle Deer, who was killed in April 1975. Durham was the last person seen with her after he picked her up from a relative's house. Eagle Deer had charged William Janklow, then-attorney general of S. Dakota (later governor) with rape.

In March 1975, lawyers working on the Wounded Knee defense committee obtained FBI files as part of court disclosures, one of which contained a report signed by Durham. When confronted, Durham acknowledged his role as a federal infiltrator. His exposure further demoralized AIM, which was then suffering under intense repression, including deaths, assaults, and imprisonment of its members.

**For More Info on these case studies:** *Agents of Repression: the FBI's Secret War Against the Black Panther Party and the American Indian Movement*, by Ward Churchill & Jim Vander Wall, South End Press, 1990 edition.

# 11. Case Studies of Informants & Infiltrators

## Quebec, FLQ Infiltrator

In the 1960s and early '70s, the Quebec Liberation Front (FLQ) carried out urban guerrilla struggle. Carole de Vault was a young Parti Qebecois activist, a sovereigntist group that shared a similar goal to the FLQ of independence. She was drawn to the FLQ's struggle, but then became a paid informant. Her real activism was with the reformist PQ; she disagreed with the militant FLQ actions since it threatened the 'legitimate' work of the PQ. This is an example of an informant that both infiltrates a group but is at the same time an activist-turned informant.

## Germinal Arrests, 2001

The arrests of the militant group 'Germinal' on their way to the anti-Free Trade Area of the Americas protests in Quebec City, April 2001, was the end of a months-long undercover operation. The group, based in Montreal, were the target of a police operation based on surveillance that indicated that one member of the group was looking for a job.

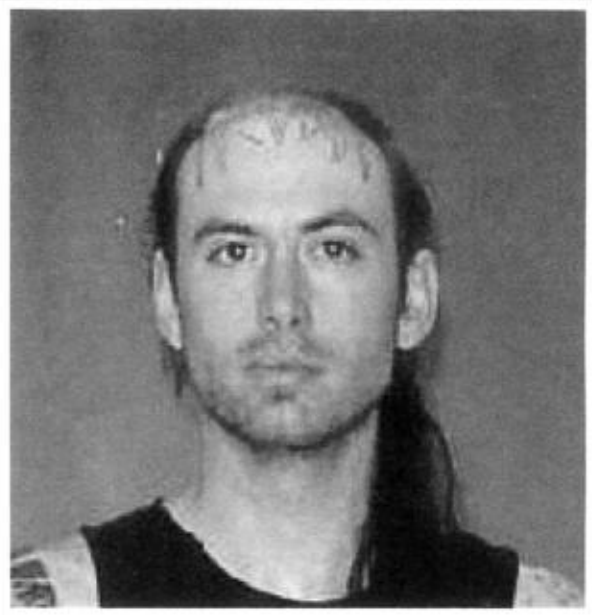
Police set up a fake furniture moving company, complete with office and trucks, staffed by undercover police agents, and postered the neighborhood where the member resided. He applied, and for several months worked alongside a police agent who eventually infiltrated the group.

Their arrests were on the eve of the mass protests of April 20-22, and were the focus of intense media coverage which police used to further justify their massive security operation. Those arrested were caught with gas masks, smoke grenades, and Thunderflashes (a powerful 'firecracker' used by the military as a grenade simulator during training). Despite this, police and media portrayed them as an 'armed group'.

This example shows how police with huge budgets for major security operations can invest tens of thousands of dollars for high-profile arrests of low-level militants.

## Operation Backfire: FBI Arrests of ELF, 2004-2006

In 2004, the FBI launched Operation Backfire, merging seven investigations in its Portland, Oregon, office. These involved 16 different attacks carried out by the Earth Liberation Front (ELF) between 1996-2002 throughout the western US that caused over $80 million in damages.



FBI hippy Informant Jacob Ferguson

In December 2005 & January 2006, the FBI indicted five women and six men on a total of 65 charges, including arson, use of destructive devices, conspiracy, and destruction of an energy facility. One prisoner killed himself while in custody. These arrests were primarily the result of one single informant: Jacob Ferguson.

Ferguson had participated in some of the ELF actions under investigation and provided the FBI with the names of others that were involved. He wore recording devices to catch them making incriminating statements about the actions. Based on these, search warrants were issued for homes and businesses, where the FBI siezed computers, manuals, fake ID's, clothing, tools and other equipment that were subjected to forensic investigations.

Ferguson was reportedly a long-time heroin addict who began collaborating with the FBI in 2004. Despite his addiction he appears to have had the trust & confidence of the group, who spoke openly with him about illegal actions while he secretly taped them.

# 12. Security Guidelines

**1. Establish security guidelines** appropriate for your group's level of activity. No collaboration with police or intelligence agencies is a good starting point. No discussion of illegal activities in any public meeting or space. Keep control of access to keys, files, funds, equipment, etc. within the hands of trusted members. Make duplicates of important files/info, etc., and store at a safe & secret location. Set up a group of trusted members who others can go to with concerns about security, police infiltration, informants, etc.

**2. Deal openly & directly** with the form and content of what anyone says or does, whether the person is a suspected agent, has emotional problems, or is simply naïve.

**3. Be aware of *Agents Provocateurs* & criminal elements** who constantly advocate risky illegal actions, and who may also have access to weapons or other resources they want to share with the group. Many groups in the 1960s-70s clearly compromised basic principles in order to accommodate this type of infiltrator.

**4. Don't accept everything you hear or read as fact.** Check with the supposed source of the information before you act. Personal communication between estranged members could have prevented or limited many FBI operations in the 1960s-70s.

**5. Do not pass on harmful rumours** about others—talk to trusted friends (or group members responsible for dealing with covert intervention). Avoid gossip about others, especially over telecommunications.

**6. Verify & double-check all arrangements** for housing, transportation, meeting rooms, etc., to ensure they have not been cancelled or changed by others.

**7. Document all forms of harassment**, burglary, assaults, raids, arrests, surveillance, attempts to recruit informants, etc. to identify patterns and targets. These can also be used for reports and legal defense.

**8. Do NOT talk with any police or intelligence agents.** Do NOT allow them into any residence without a warrant. Try to get fotos of agents involved. If naïve members do engage in conversations with police or agents, explain the harm that could result.

**9. Alert others if police or intelligence harassment increases**, (hold meetings, make press releases, etc.). This makes other groups aware of repression and can limit further harassment through exposure.

**10. Prepare group members to continue organizing** if leaders are arrested, etc. This includes sharing knowledge & skills, public contacts, etc.

# Resist the System of Surveillance & Social Control

***Above:*** Members of Canadian military Joint Task Force 2. ***Below:*** Surveillance cameras in London, England



# Fight For Freedom!



*[For photocopying purposes, print out at 600 dpi]*

**RESIST-RESIST- RESIST THE POLICE STATE!!!**