Resist the System of Surveillance & Social Control


Fight For Freedom!
RESIST-RESIST- RESIST THE POLICE STATE!!!

Security & Counter-Surveillance

Information Against the Police State

Revised & Updated:
New Surveillance Technology & Techniques
New Section on Informant & Infiltration Operations
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 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...
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 by 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. His background was based on his experience with weapons & violence.
In order to stop the Panther/Blackstone Ranger alliance, 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 & the location of his head-shooting.
On December 4/69, fourteen heavily armed police raided the apartment using a warrant for “illegal weapons.” Earlier that day, O’Neal had made contact with 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 .45 (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 bodyguard was hiding, killing him 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’Neal reportedly killed himself in the 1980’s)

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. In order to be successful, it is essential to learn the various sources that is subjected to analysis & comparison, is called intelligence. The gathering of intelligence is a vital part of counter-insurgency operations. For this reason, the enemy does not know who, what, where or when to strike.

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 even ten operators in six vehicles (or even more, of course). In addition, motorcycles, bicycles, 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 photographic 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, conversations, personal relationships, etc. More generally, it consists of various 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 surveillance can be directed. 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 that would lead to secret information.

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 being in service.
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 signs. They will also stop the flow of information. For this reason, surveillance can be difficult to detect because it is subtle & covert.
Designing & conducting 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 resident 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).

4. Other harassment

Other forms of harassment used by the FBI & police included:...

5. Physical Surveillance

Physical surveillance is carried out by enemy personnel (operators) on foot 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 ‘floating boxes’ (in front, the back, sides, and on parallel routes).

If physical surveillance is being carried out, then it can be assumed that technique is also being used, and may have been for some time before physical surveillance began. This is because physical surveillance requires multiple operators if it is to be successful, and can be draining on personnel and resources. Therefore, while it is likely 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 elderly members of the community (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 behavior that should be monitored.

In order to coordinate the efforts of many team members, communications body gear is worn by operators. This usually consists of clear plastic capes 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 drained movements of time & resources, diverting them from other forms of struggle.

Appearance of any model, year, condition, colour, etc. may have been for some time before physical surveillance began. This is because physical surveillance requires multiple operators if it is to be successful, and can be draining on personnel and resources. Therefore, while it is likely that surveillance operators may have access to audio recordings of the target’s conversations in a residence or vehicle, while they are observing them.

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, and the location of the target. When a mobile surveillance is performed, a fixed surveillance of a target expected to appear at the location (zakou'i) is used. 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 turn into mobile surveillance with operators pre-positioned and ready to follow.

7. Other harassment

Other forms of harassment used by the FBI & police included:....
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 liberalization 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 nationwide, 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 some in 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 on generating 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 the 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 TrPeten (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 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 &/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, & 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.

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.

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 practice, 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 towers, 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 communications 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 without your knowledge. 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 can monitor listening devices on your computer. These methods have been used to arrest people making internet threats. In some cases, police identify an IP address then acquire video from internet access points to investigate 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).

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 airplanes to receive transmissions when it wasn't possible to get a ground vehicle close enough to a hidden transmitter (worn by an informant). Buildings & public areas can transmit conversations, 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.

Parabolic Microphones
Powerful microphones are designed to eavesdrop on conversations over a long distance. Also referred to as a "bionic ear" or "stereophone". These 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 up to 300 metres. Civilian versions are sold for bird watching, and some attach to binoculars (which will have a small boom microphone sticking out). 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 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 x's will be behind your back. Activists must 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 first name so he/she doesn't forget to respond to their name), and a skeleton of personal history, such as a business owner or military man who will vary the sound-and-work 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 will 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."

Informant-Handler Meetings
As part of an undercover operation, the infiltrator/informant must exchange information, equipment or money with their handler. The most secure method for 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, records, 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 phone. The agents had access carried out counter-surveillance." (Hells Angels: Into the Abyss, by Yves Lavigne, Harper/Collins Publishers Ltd., Toronto 1996, pp. 237-38)

When they had to communicate over telephone, one would phone the other's pager and use a phone number they could be reached at. Even then, their conversations were limited to 100 words.

"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, McKinley 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 they are extremely good at it). We play the game of knowing members 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 and learn more about their own informants & infiltrators.Unless there is strong evidence, public accusations & denouncements can sometimes cause more damage than good. They may appear as overly paranoid, personal attacks/divisiveness, 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, attack the group, the risks, sacrifices, and what they feel is the 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 informant? 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 that they are spies."

"What are a person's means of living? Who are her or his friends? What sorts of contradictions exist between their professorial 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 bikers' counterintelligence, which involved extensive background checks, failed to uncover their true identity. Private investigators hired by the bikers with other intelligence sources, only reaffirmed the fake ID's of the agents, and provided a false sense of security to the gang.
A standard method of recruiting informants is to find people (in or near the group) with problems. Persons most inclined to cooperate 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). Informants, of course, 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, university-CCTV cameras are available for intelligence agencies in general. Informants may also identify themselves as undercover agents 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 agents provocateurs (an informant or agent who provokes actions, usually illegal and which lead to arrests). Informants are civilians recruited by the state security forces (or corporations), or police infiltrators. 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).

Informants 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. The informant may befriend one member in order to gain contact with the entire group. Informants can also enter a group as genuine members from another area or region, where they first made contact with the movement. They may 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, university-CCTV cameras are available for intelligence agencies in general. 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 COMTEIL-PRO Techniques).

Types of Informants

- The "hang around" type: they are persons who regularly show up 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, key leaders or 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.

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. For surveillance operations, miniature CCTV video cameras are also routinely used. They have filmed people making suspicious phone calls, purchasing 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 camera

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 listening device, the power source may be a battery or it may be directly wired to a residence or vehicle power supply. Sophisticated video cameras can have an extended life when left out in the open.

In cases where physical surveillance of a suspect was either too difficult, or illegal activities occurred at too long an interval, CCTV video cameras have been covered up or set 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 two years (i.e., whereas when physical surveillance would be largely unproductive).

Powerful video cameras are also mounted on helicopters, planes and Unmanned Aerial Vehicles (UAV). These have been used to monitor the homes of persons suspected of carrying out sporadic attacks over the course of two years (i.e., whereas when physical surveillance would be largely unproductive).

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. These days, digital cameras are ubiquitous. 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. Various CCTV cameras & 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 computer-intelligence device 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.

Commercially-available tracking devices, such as the Quickpass 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 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 purposes (to prevent victims of kidnapping).

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.

Night-Vision & Thermal Imaging

Night-vision devices (NVD's) magnify existing moon & star light, allowing the viewer to see in what would otherwise be total darkness. They provide a high contrast 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, hundreds of goggles, recently used by firefighters, dug up by earth, etc. can all be detected. Specialized thermal imaging equipment can also be used to monitor the movement of people inside a structure.

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 widespread.

Aerial Surveillance & Night Vision

To evade aerial surveillance go inside malls, apartment buildings, transit stations, or any building that has multiple exits.

Great care & planning should be put into any anti-surveillance action, and disguises must be effective. Consideration should also be given to the movements of other surveillance teams.

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 much more 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 evade surveillance. For example, targets moving on foot can exploit terrain & routes of travel to break up or evade surveillance. 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, arrest, 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.
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 that is 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 CleanDisk Security and PGP.

4. Encrypt any sensitive data on your computer, CDs or floppy disks using a programme such as PGP (or GPG). Ideally, you will stuff all files into one big archive (eg using WinZip or StuffIt) and encrypt that. This means that even if 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 – 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- up at home.

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/sensitive 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 your privacy use PGP encryption (www.pgp.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 know 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 need to include a PGP encryption (www.pgp.com). Don’t do anything in an email you would not be prepared to justify in court.

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 web-sites contained in unsolicited emails 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 know 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 need to include a PGP encryption (www.pgp.com). Don’t do anything in an email you would not be prepared to justify in court.

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, such as BluffTitler (www.blufftitler.com). 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].

   WorldTracker GPS tracker, commercially available

Listening Devices/Mini-Cameras

1. To protect against covert entry & placement of devices in a residence, vehicle, standard antiburglar 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.

   Some 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 informers. 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.

2. Encrypted voice-activated devices can greatly assist in retention & the ability to later identify the same individual or vehicle.

   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 as used as a back up reciever.

   To counter listening devices, bikers began using dry- erase or chalk-board to write down secret information, then erase 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.

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

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

   Code: letter-number key. Choose a ten letter word in which no ‘i’ or ‘o’ appears and then assign a number to each letter: J M B R W 1 2 3 4 5

4. Example: V O R T R E 9 = W B N A

   Code on phone: the black singer

Tracking Devices

1. To counter the use of tracking devices, do not use miniaturized 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 the vehicle or place 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].

   WorldTracker GPS tracker, commercially available

2. 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, such as BluffTitler (www.blufftitler.com). 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].

   WorldTracker GPS tracker, commercially available

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, such as BluffTitler (www.blufftitler.com). 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].

   WorldTracker GPS tracker, commercially available

4. 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, such as BluffTitler (www.blufftitler.com). 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].

   WorldTracker GPS tracker, commercially available

5. 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, such as BluffTitler (www.blufftitler.com). 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].

   WorldTracker GPS tracker, commercially available

6. Group characteristics of Surveillance Operators (Foot & Vehicle):

   ● If a vehicle is used, this could be used as evidence of guilt, to either a particular individual or ethnicity, any size or shape, young or old.

   ● They may appear out of place, nerves & tense (because they are).

   ● They can hand devices over to you, 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 effective at 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 are possible potential operators. Some times, 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, or camper home, or cable truck—large enough to contain operators & surveillance equipment. Like the apartment scenario, a vehicle OP will be marked by its lack of activity 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 in or near a public place to record a heartbeat 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 will act normal (even if they are a known 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 (without being noticed) 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 to operators which reveal their activity. Some of this is subconscious and becomes part of the routine of surveillance operators.

For example, mirroring is when a surveillance operator duplicates your actions as they follow your lead, especially in vehicle surveillance. Pace is when they keep 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.

Moving through channelized terrain, operators may be forced to use rear-view mirrors. Wrap-around sunglasses can also aid in surveillance. The best is when a surveillance operator can use rear-view mirrors. Wrap-around sunglasses can also aid in surveillance. The best is when a surveillance operator can observe for possible surveillance. Leaving and then returning for sitting or sleeping, as well as tracks, litter, equipment dragged by operators, etc. Knowledge of tracking can greatly assist in identifying potential OP sites. Longer term OPs 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. They determine the best locations and types of devices to be used. They then leave, prepare technical 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 strangely or leave a target area unexpectedly to control them during the course of a 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 nights or unexpected gifts such as stereos or TV’s (trojan horse). Surveillance using technical means is a natural extension 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. It will quickly u-turn as well & resume the follow. A well-trained phone connections. Devices can be re-attached to another vehicle, etc.

In enclosed spaces such as rooms & vehicles known to police-intelligence agents, or on any telecommunications, it is almost impossible to secure against technical surveillance. When personal 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 romans, 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 Activity & Campaign, a publication from resistance in the UK (www.ActivistSecurity.org). Overall, however, all telecommunications should be considered insecure forms of communicating.