

The Anarchist Library
Anti-Copyright



Security Culture

a handbook for activists

securitysite@tao.ca

securitysite@tao.ca
Security Culture
a handbook for activists
2001

Retrieved on 2020-08-15 from
[https://warzonedistro.noblogs.org/files/2017/09/
security_culture_handbook.pdf](https://warzonedistro.noblogs.org/files/2017/09/security_culture_handbook.pdf)

theanarchistlibrary.org

2001

9. IF YOU ARE NERVOUS ABOUT SIMPLY REFUSING TO TALK, YOU MAY FIND IT EASIER TO TELL THEM TO CONTACT YOUR LAWYER. Once a lawyer is involved, people will know more about your state i.e. charges, bail, court date, etc.

3. IF THE POLICE DO PRESENT A WARRANT, YOU DO NOT HAVE TO TELL THEM ANYTHING OTHER THAN YOUR NAME, ADDRESS AND BIRTH DATE. Carefully observe the officers; you're in your own home you're not required to stay in one room. You should take written notes of what they do, their names, badge numbers, and what agency they're from. Have friends who are present act as witnesses. It's risky to let cops roam around alone in your place.
4. IF THE POLICE TRY TO QUESTION YOU OR TRY TO ENTER YOUR HOME WITHOUT A WARRANT, JUST SAY NO. The police are very skilled at getting information from people, so attempting to outwit them is very risky. You can never tell how a seemingly harmless bit of information can hurt you or someone else.
5. ANYTHING YOU SAY TO THE POLICE MAY BE USED AGAINST YOU AND OTHER PEOPLE. Once you've been arrested, you can't talk your way out of it. Don't try to engage cops in a dialogue or respond to accusations.
6. YOU DO NOT HAVE TO REVEAL YOUR HIV STATUS TO THE POLICE OR JAIL PERSONNEL. If you've been arrested you should refuse to take a blood test until you've been brought before a judge and have a lawyer of your choice.
7. YOU HAVE A RIGHT TO TELEPHONE A LAWYER OF YOUR CHOICE AS SOON AS POSSIBLE. This means after you've been arrested, charged and booked into jail. This does not mean however, that you'll be given the right to speak with your family and friends. This is left up to the discretion of the police involved in your case.
8. LYING TO THE POLICE IS A CRIME.

Contents

Introduction	5
Security Culture: What it is, why we need it and how to implement it...	6
Activism and State Repression	6
So What is a Security Culture?	7
(In)Secure Practices	8
What Not To Say	8
Three Exceptions	9
Security Measures	10
Security Violating Behaviours	10
Educate to Liberate	12
Dealing with Chronic Security Problems	13
a brief primer on the canadian state security apparatus	13
An Overview of Domestic Intelligence Organizations	15
<i>The Golden Rule of Silence</i>	17
The Counter-Insurgency Model	18
everything you ever wanted to know about informers and infiltrators	19
Who is an Informer?	19
Background Checks — An Essential Tool	22
The Unwitting Informer	23
Know Your Own Limits	24
Covert Action Other Than Infiltration	25
Moving Against Informers: Considerations and Alternatives	27
Your Rights	29

certainly the group's responsibility to quietly contact leadership in other groups to warn them about the agent. Often public exposure is done through the group's newspaper/newsletter/journal; in this case, the news article should be sent to a wide variety of groups. The more pressing problem is the instance where there are only suspicions but not decisive evidence.

Experience has shown that suspicions are taken seriously only when there is a political bond that exists between persons with long movement experience. People who have been in the movement a long time, and who are known to each other and trusted as dedicated movement people, can convey agent suspicions that will get a favorable hearing or be readily believed. This "old hands trust network" is relatively independent of political point of view; veteran leaders of rival radical organizations can freely and easily exchange information on matters of security.

Your Rights

1. **YOU DON'T HAVE TO TALK TO THE POLICE OR INVESTIGATORS.** You do not have to talk to them on the street, if you've been arrested, or even if you're in jail. Do not talk about illegal actions with fellow "inmates" in holding as they may be plants.
2. **YOU DON'T HAVE TO LET CSIS OR THE POLICE INTO YOUR HOME OR OFFICE UNLESS THEY HAVE A SEARCH OR ARREST WARRANT.** Demand to see the warrant. It must specifically describe the place to be searched and things to be seized. It must be authorized by a judge and should bear a signature.

2. doing nothing outwardly but continuing the investigation;
 3. isolating the person from sensitive work but keeping him or her in the group;
 4. moving to a higher stage of investigation.
- c. What will be done If the person does turn out to be an agent? While common sense dictates that the person be exposed and severed from the group, other actions might be initiated. If the presence of the agent is a real threat to the group, then the agent should be neutralized in an effective manner. Usually wide exposure of the agent will accomplish an effective neutralization. But if the agent is no great threat to the group's functioning, the agent staying inside the group may be useful for other purposes.

The group might decide that they prefer to keep the agent, rather than risk not knowing who would replace a known quantity. If the agent is not in a sensitive position, can be monitored and isolated from important work, the group may want to keep such an agent at a low organizational level. Or the agent might be given tasks that seem to be sensitive but are in reality not crucial to the group. Under the cover of doing "sensitive" work, false and semi-false information about the group can be relayed to the intelligence agencies that the agent belongs to. Or perhaps certain information that is in fact true about the group can be willfully discredited by creation of pseudo-events and/or false information. Remember that when the intelligence agencies have a great deal of contradictory information, it decreases their ability to act decisively against the group.

- d. What are the responsibilities to other groups of the group's knowledge of an informer? If the group makes a decision to sever connection with the agent it is

This handbook is the third edition of what we have been an evolving and growing document dealing with security issues and Canadian activism. We would like to say a big thanks to the Collective Opposing Police Brutality in Montreal for editing some of the text of the original pamphlet and adding so many great examples to the Informants and Infiltrators section. We have replicated many of their changes in this edition. Thanks also goes out to Eric Drooker whose artwork we used throughout this pamphlet.

For more information or to make contributions to this document — please email securitysite@tao.ca

Third edition — prepared November 2001.

Introduction

Resistance has been on the rise for the past few years, with activists adopting more and more effective tactics for fighting back. Our increased activity and effectiveness has meant that the RCMP, FBI, and local police have continued to escalate their activities against us. As well, the events of September 11th and ensuing state hysteria are no small footnote to the way that our radical and revolutionary movements have and will be targeted by repressive state forces.

If we want our direct action movement to continue, it is imperative we start tightening our security and taking ourselves more seriously. Now is the time to adopt a security culture. Good security is certainly the strongest defense we have.

This is a handbook for the Canadian activist who is interested in creating and maintaining security awareness and culture in the radical movements. We are always looking for contributions — so please feel free to email securitysite@tao.ca with any images or text you think belong in a handbook such as this.

This is the third edition of this zine that we have put out in order to add and improve on the original text (thanks for the work of the Collective Opposing Police Brutality in Montreal for their help). There will be future editions of this handbook so keep putting forward suggestions to us.

We hope that you will put the material contained within to good use. Now more than ever is the time to act!

Security Culture: What it is, why we need it and how to implement it...

Activism and State Repression

This pamphlet has essential information for anyone associated with groups advocating or using economic disruption or sabotage, theft, arson, self-defence from police or more militant tactics. The advice that follows also applies to anyone associated with groups practising civil disobedience, especially since people often work in several groups at the same time and gossip travels freely between them.

Even if you've never expressed your politics by doing property damage, pitching cobblestones, or getting arrested for civil disobedience; even if you think you have nothing to hide, these guidelines are presented here to enhance your personal safety as well as the overall effectiveness of our movements.

The simple reality is that governments in industrialized countries target groups that advocate economic sabotage and groups that don't, movements that are militant and movements that are markedly pacifist. The government's security machinery serves the elitist political and economic objectives of capitalism. There are over 250 political prisoners in Canada and the US that can testify to this from first-hand experience. By adopting a security culture, we can limit or neutralize

Moving Against Informers: Considerations and Alternatives

(Taken from PROTECTING OURSELVES FROM STATE REPRESSION: A MANUAL FOR REVOLUTIONARY ACTIVISTS. Published in 1984 by the Anti-Repression Resource Team — Jackson, Mississippi)

Assuming that the security people within the group have suspicions about a group member being an informer/provocateur, it is useful for security/leadership to resolve certain questions both before and after the investigation:

- a. How badly do you want to know whether the person is in agent or not? Clearly, if the person under suspicion is relatively important to the group's functioning, then leadership must know one way or the other. The more important the person under suspicion is to the group, the more intensive the investigation. We may suggest methods of investigation which are unorthodox and from a certain point of view morally indefensible. But the question is always how badly the group needs to know. No group need use all or any of the methods we describe. But under the condition that the correct information is a life-and-death matter for the group, certain drastic measures may be justified.
- b. What will be done if the information is inconclusive? Often there is not enough evidence to confirm that someone is a police agent, but there IS enough evidence to confirm certain suspicions. A great deal will depend upon what is at stake with the person under suspicion. In general, the choices come down to
 1. labelling the person a security risk and acting accordingly;

black bloc members attacked demonstrators and small shops. With a lack of public information, the police help manipulate public discourse along the lines of “how do legitimate demonstrators isolate activist thugs?”

Slandorous propaganda can take the form of anonymous letters, or rumours aimed at the activist milieu. There are also examples where police will make uncorroborated, casual accusations to journalists that, to use two examples, a person is a drug dealer, or that at a demonstration, a person aimed a handgun at an officer. It is often for slanderous reasons that police charge activists with “weapons possession” for having a penknife, or charges of violence like “assault.”

The growth of the anti-globalization movement has been accompanied by renewed anarchist-scare propaganda on the part of authorities. Politicians and police attempt to massage public opinion, preparing people for a crack down, in order to legitimate the use of heavier methods of social control, exclusion and repression.

Manipulative disinformation spread through the media needs to be denounced as lies. There are activist-friendly lawyers who can help us demand retractions and corrections. Speak to the journalists involved, call them on their sloppy, dishonest work, expose their hypocrisy, and complain to the journalists’ ethics body. We can not rely on capitalist, private-media for any kind of fairness.

It is valuable for us to learn more about the covert actions of the police. There exists a long and documented history. Factual information about police covert activities also comes out as evidence presented in court. An important, too often neglected part of our strength is our knowledge of, and our protection from, police action against us.

counter-intelligence operations meant to disrupt our political organizing, be it mainstream or underground.

Peasant-rebels; communards; liberationists; abolitionists; labour organizers; revolutionaries; from large uprisings challenging the entire political structure, to isolated environmental and social struggles, people have constantly worked to create a better world. The response of government has always been repression to preserve the status quo.

Historically, government surveillance and harassment has increased relative to the ascendancy of direct action movements. Minimizing the destructiveness of political repression requires that we

implement and promote a security culture within our movements.

So What is a Security Culture?

It’s a culture where the people know their rights and, more importantly, assert them. Those who belong to a security culture also know what behaviour compromises security and they are quick to educate those people who, out of ignorance, forgetfulness, or personal weakness, partake in insecure behaviour. This security consciousness becomes a culture when the group as a whole makes security violations socially unacceptable in the group.

Security culture is about more than just targetting specific behaviours in individuals such as bragging, gossiping or lying. It is also about checking movement behaviours and practices as a whole to ensure that our own oppressive practices don’t feed into intelligence operations being carried out against our community.

For example, racism or sexism in the movement can help to spread division, make some people more open to infiltrators (those who feel marginalized by group practices), and create openings that can be used by state operatives. Obviously, our

movements have a lot of work to do before we address the bigger questions — what’s important here is to recognize how oppressive behaviours play into bad security culture overall.

(In)Secure Practices

Activists like to talk, we generally can spend hours and hours discussing theory, tactics, and strategy. Mostly this is useful in building our analysis and our work, but in other cases this can be dangerous.

What Not To Say

To begin with, there are certain things that are inappropriate to discuss. These things include:

- your involvement or someone else’s involvement with an underground group
- someone else’s desire to get involved with such a group
- asking others if they are a member of an underground group
- your participation or someone else’s participating in any action that was illegal
- someone else’s advocacy for such actions
- your plans or someone else’s plans for a future action

Essentially, it is a bad idea to speak about an individual’s involvement (past, present or future) with illegal activities. These are unacceptable topics of discussion regardless of whether it is rumor, speculation or personal knowledge.

a hell of a lot more time than your comrades, DON’T DO THE ACTION.

Make certain that you talk with others in your affinity group about situations that make you uncertain whether you should be involved in particular actions, especially those that are at a high risk of being criminalized.

Remember — there is no excuse for turning in comrades to the police — and those activists that do effectively excommunicate themselves from our movements. We must offer no legal or jail support to those activists who turn in others for their impact on our movement is farreaching and can have devastating effects.

Covert Action Other Than Infiltration

Covert (or “Special”) Action from police and secret service is also done outside of the group, with or without infiltration. These efforts include: intimidation and harassment, blackmail and manipulation, propaganda, informing employers and security checks, as well as physical sabotage like theft and arson.

Intimidation and harassment can include visits from secret service agents, calling you or your partner by their first name on the street, thefts where obvious clues are left. Police will try to blackmail people if they want to recruit or neutralize them.

Police uses propaganda in an attempt to poison the atmosphere and manipulate media and public opinion. In December 1971, when the FLQ was near its end and heavily infiltrated, the RCMP issued a false FLQ communiqué in the name of the “Minerve” cell. The communiqué adopted a hardline position, denouncing the abandonment of terrorist action by a well-known activist, Pierre Vallières, and urging the continuation of armed struggle.

In Genoa, Italy, police played an active covert role in trying to discredit black bloc anarchists during the July 2001 meeting of the G8. Several reports reveal that Italian police masked as

hear of it. These activists don't mean to do harm, but their bragging can be very damaging.

It is your responsibility to instruct these people on the importance of security culture.

The other type of activist-informer is the person who cracks under pressure and starts talking to save his or her own skin. Many activists get drawn into situations they are not able to handle, and some are so caught up in the "excitement" that they either don't realize what the consequences can be, or they just don't think they'll ever have to face them.

Keep in mind that the categories of "planted informer" and "activist-turned-informer" can, and have been blurred. In 1970, during the height of the FLQ's activities, Carole de Vault — a young Parti Quebecois (PQ) activist was drawn to the FLQ, but then became a paid police agent. Her "activism" was with the PQ; she disagreed with the heavier FLQ actions since it threatened the "legitimate" work of the PQ. Her involvement with the FLQ was as a planted police informer.

Know Your Own Limits

We have to know the possible consequences of every action we take and be prepared to deal with them. There is no shame in not being able to do an action because of responsibilities or circumstances that make it impossible for you to do jail time at this point in your life. As long as capitalism and all of its evils exist, there will be resistance. In other words, there will be plenty of great actions for you to participate in when your life circumstances are more favourable.

If others are dependent on you for support, you aren't willing to lose your job, or drop out of school or ruin your future career, DON'T DO THE ACTION. If you are addicted to an illicit drug and/or have a lengthy criminal record, the cops will use this to pressure you for information. If you don't feel capable of detoxing under interrogation and brutality, or doing

Please note: this is not to say that it is incorrect to speak about direct action in general terms. It is perfectly legal, secure and desirable that people speak out in support of mokey-wrenching and all forms of resistance. The danger lies in linking individual activists to specific actions or groups.

Three Exceptions

There are only three times that it is acceptable to speak about specific actions and activist involvement.

The first situation would be if you were planning an action with other members of your small group (your "cell" or "affinity group"). However, these discussions should never take place over the Internet (email), phone line, through the mail, or in an activist's home or car, as these places and forms of communication are frequently monitored. The only people who should hear this discussion would include those who are actively participating in the action. Anyone who is not involved does not need to know and, therefore, should not know. The second exception occurs after an activist has been arrested and brought to trial. If s/he is found guilty, this activist can freely speak of the actions for which s/he was convicted. However, s/he must never give information that would help the authorities determine who else participated in illegal activities. The third exception is for anonymous letters and interviews with the media. This must be done very carefully and without compromising security. Advice on secure communication techniques can be found at <http://security.tao.ca>.

These are the only situations when it is appropriate to speak about your own or someone else's involvement or intent to commit illegal direct action.

Security Measures

Veteran activists only allow a select few to know about their involvement with direct action groups. Those few consist of the cell members who they do the actions with AND NO ONE ELSE!

The reason for these security precautions is obvious: if people don't know anything, they can't talk about it. When activists who do not share the same serious consequences know who did an illegal direct action, they are far more likely to talk after being harassed and intimidated by the authorities, because they are not the ones who will go to jail. Even those people who are trustworthy can often be tricked by the authorities into revealing damaging and incriminating information. It is safest for all cell members to keep their involvement in the group amongst themselves. The fewer people who know, the less evidence there is in the long run.

Security Violating Behaviours

In an attempt to impress others, activists may behave in ways that compromise security. Some people do this frequently — they are habitually gossiping and bragging. Some activists say inappropriate things only when they consume alcohol. Many activists make occasional breeches of security because there was a momentary temptation to say something or hint at something that shouldn't have been said or implied. In most every situation, the desire to be accepted is the root cause.

Those people who tend to be the greatest security risks are those activists who have low self-esteem and strongly desire the approval of their peers. Certainly it is natural to seek friendship and recognition for our efforts, but it is imperative that we keep these desires in check so we do not jeopardize the safety of other activists or ourselves. People who place their desire

engage in have been discussed on an abstract basis. If there is a strong basis for believing this person might be interested in the action, then the general idea of an action can be run by them. Only when they have agreed to participate, do they come to the group to discuss action details.

During the trials of activists, police often reveal the kinds of information that they have gathered concerning our groups and activities. Note what revelations come out of these trials. What are the possible and likely sources of the information? Speak to persons that have been arrested and interrogated to see what they may have said to the police, or discussed in their jail cell.

Placing infiltrators in social justice and revolutionary movements is an established practice. It was done to the Black Panthers, AIM, the Front de Libération du Québec (FLQ), and the peace/ anti-war/and anti-nuclear movements on a large scale. Small groups, such as affinity groups, or working groups of larger more open organizations, need to be especially careful with new members. Direct action organizing is ideally done with longstanding, trusted members of the activist community.

This doesn't mean that no one else should ever be allowed into these groups. On the contrary, if our movement is to continue to grow, new people should be welcome and recruited; we just need to keep security in mind and exercise caution at all times.

The Unwitting Informer

Possibly an even greater threat to our movements than the covert operative is the activist-turned-informer, either unwittingly or through coercion.

The unwitting informer is the activist who can't keep his/her mouth shut. If someone brags to you about what they've done, make sure this person never has any knowledge that can incriminate you, because sooner or later, the wrong person will

pany and specifically poster opportunities for employment in the vicinity of a Germinal member seeking employment.

The trap worked. Tipped off by an initial informant, two under-cover cops worked for four months in the group. This operation resulted in the media-hyped “dismantlement” of the group on the eve of the summit. Seven Germinal members were arrested, 5 of whom spent 41 days in preventive custody, only to be released under draconian bail conditions.

The police’s covert action was in part about dismantling the group, but it was also about creating a media/propaganda campaign to justify the police-state security for the summit.

Background Checks — An Essential Tool

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? One of our strengths as activists is our ideas and values, our counterculture, our attitudes towards the dominant society. Our sincerity in discussing these things is also a way of learning about each other.

When planning for new actions, care must be taken concerning who is approached. As little as possible should be said about the actual action plan until a person’s political philosophy, ideas about strategy, and levels of risk they are willing to

for friendship over the importance of the cause can do serious damage to our security.

The following are examples of security-violating behaviours:

Lying: To impress others, liars claim to have done illegal actions. Such lies not only compromise the person’s security — as cops will not take what is said as a lie — but also hinders solidarity and trust.

Gossiping: Some people think they can win friends because they are privy to special information. These gossips will tell others about who did what action or, if they don’t know who did it, guess at who they think did what actions or just spread rumors about who did it.

This sort of talk is very damaging. People need to remember that rumors are all that are needed to instigate an investigation or even lay charges.

Bragging: Some people who partake in illegal direct action might be tempted to brag about it to their friends. This not only jeopardizes the bragger’s security, but also that of the other people involved with the action (as they may be suspected by association). As well the people who s/he told can be charged as accessories after the fact. An activist who brags also sets a bad example. Indirect-Bragging: Indirectbraggers are people who make a big production on how they want to remain anonymous, avoid protests, and stay “underground.” They might not come out and say that they do illegal direct action, but they make sure everyone within earshot knows they are up to something.

They are no better than braggers, but they try to be more sophisticated about it by pretending to maintain security. However, if they were serious about security, they would just make up a good excuse as to why they are not as active, or why they can’t make it to the protest. Concealing sensitive information from even trusted comrades is far better than jeopardising underground work.

Educate to Liberate

The unfortunate truth is there are some security-ignorant people in the movement and others who have possibly been raised in a “scene” that thrives on bragging and gossiping. It doesn’t mean these people are bad, but it does mean they need to inform themselves and learn about personal and group security. Even seasoned activists make mistakes when there is a general lack of security consciousness in our groups.

And that’s where those of you who are reading this can help. We must ALWAYS act to inform persons whose behaviour breaches security. If someone you know is bragging about doing an action or spreading security-compromising gossip, it is your responsibility to explain to her or him why that sort of talk violates security and is inappropriate.

You should strive to share this knowledge in a manner that encourages the person’s understanding and changes her/his behaviour. It should be done without damaging the person’s pride. Show your sincere interest in helping him/her to become a more effective activist. Keep your humility and avoid presenting an attitude of superiority. An insensitive approach can raise an individual’s defences and prevent them from listening to and using the advice offered. The goal of addressing these issues with others is to reduce insecure behaviour, rather than showing how much more security-conscious you are.

Share your concerns and knowledge in private, so that the person does not feel as if they are being publicly humiliated. Addressing the person as soon as possible after the security violation increases effectiveness.

If each of us remains responsible for discussing security information with people who slip up, we can dramatically improve security in our groups and activities. When people recognise that lying, gossiping, bragging, and inappropriate debriefing damages both themselves and others, these behaviours will soon end.

tion 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 shunned and kept away from the movement.

Some types of infiltrators stay in the background and offer material support, other informants may have nothing to do with the group or action, but initially heard certain plans and tipped off the police. Among the more active types of infiltrators can be a gregarious person that quickly wins group trust. Some infiltrators will attempt to gain key forms of control, such as of communications/ secretarial, or finances. Other informants can use charm and sex to get intimate with activists, to better spy or potentially destabilize group dynamics.

Active infiltrators can also be provocateurs specializing in disruptive tactics such as sowing disorder and demoralizing meetings or demos, heightening conflicts whether they are interpersonal or about action or theory, or pushing things further with bravado and violent proposals. Infiltrators often need to build credibility; they may do this by claiming to have participated in past actions.

Also, infiltrators will try to exploit activist sensibilities regarding oppression and diversity. Intelligence organizations will send in someone who will pose as a person experiencing the common oppression of the particular activist group. For example, in the 1960’s, the Weather Underground (“Weathermen” — a white anti-imperialist armed struggle in the US) was infiltrated by an “ordinary Joe” informant with a working class image. Black war veterans infiltrated the Black Panther Party.

A fresh example of police infiltration and manipulation tactics is that of Germinal, a group targeted for arrest two days prior to the April 2001 anti-FTAA demonstrations in Quebec City. Five months prior, the police set up a false transport com-

Let's discuss the deliberate informers first. They are often difficult to identify. Informers can be of any age and any profile, but they do have a few discernible methods or operation, or "modus operandi." These are:

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 initiatives, 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 ac-

By developing a culture where breaches of security are pointed out and discouraged, all sincere activists will quickly understand.

Dealing with Chronic Security Problems

So what do we do with activists who repeatedly violate security precautions even after being informed several times?

Unfortunately for them, the best thing to do is to cut them loose. Discuss the issue openly and ask them to leave your meetings, basecamps and organizations. With law enforcement budgets on the increase, new anti-terrorist laws that call for stiffer sentences for political actions, and with courts handing down long sentences for political "crimes," the stakes are too high to allow chronic security offenders to work among us.

By creating a security culture, we have an effective defence against informers and agents who try to infiltrate groups. Imagine an informer who, every time they ask another activist about their activities, receives information about security. It would frustrate the informer's work. When other activists discovered that she/he continued to violate security precautions after being repeatedly informed, there would be grounds for isolating the person from our groups. And that would be one less informer for us to deal with!

a brief primer on the canadian state security apparatus

Recent incidents of repression against activists in British Columbia illuminate the need for grassroots people to understand and practice movement security. Police monitoring, infiltration and agent provocateurs are routinely used by the state to collect information about our groups, or specific individuals in them, and to subvert our activities.

For example, during the APEC hearings, it was revealed that over seventy groups and individuals were monitored before and during the APEC meetings in 1997. A paid industry informant/disruptor was identified at a wilderness action camp in 1999. Provocateurs also targeted some Vancouver activists, trying to convince them to disclose information and as well, to break the law.

The Canadian security apparatus identifies a number of our groups and activities as a threat to “national security.” People and organizations are widely targeted; even avowed pacifists have been included in surveillance and repressive measures. According to the Canadian Security and Intelligence Service’s (CSIS) annual reports, activities targeted in the late 1990s included: native resistance, environmental & animal rights movements, anti-poverty, anti-globalization, anti police brutality, anti-racist, anarchist and communist groups.

With the rise in militant First Nations’ struggles; covert direct action against corporations; the renewed militancy and strength of popular struggles; and the mass-media’s increasing focus on anarchists and anti-globalization protests, there is also a growing level of police surveillance and repression.

The need for security in our movements is obvious — however, it is incredibly important that we don’t fall into the trap of using our awareness of security issues to shut other people out of our growing movements.

One of the key aims of the FBI’s Counter-Intelligence Program (“COINTELPRO”) operations against the Black Panthers and American Indian Movement (AIM) was to spread distrust and paranoia so that these activists would be reluctant to integrate new people into their struggles.

A security culture *can* exist in a large movement; indeed, it is one indication of a movement’s strength. Arming ourselves with knowledge about how the system works and works against activists is essential in building security culture. The aim of this section is to give a brief run down of the working

practice security at all points in the movement’s development. State agents gather more than just “hard evidence;” they are interested in knowing about radicals’ beliefs as well.

Police try to control with fear; don’t be intimidated. Remember — **If an agent comes knockin’, do no talkin’.**

everything you ever wanted to know about informers and infiltrators

Infiltrators seek information on most radical groups. The return of mass mobilizations and radical actions in anti-globalization, anti-poverty, anti-racism and anti-police brutality demonstrations, as well as declarations to continue struggling in the streets and underground has drawn attention from the state’s secret police. More infiltrators will be sent into our ranks to try to bribe, entice or manipulate individuals. The extent to which they are able to infiltrate our groups depends on our seriousness and responsibility in learning about, promoting, and working within a security culture.

Radical movements can learn to better identify covert enemies in our projects. Once identified, appropriate action is needed to undo, contain, or remove the danger.

This section is intended to arm you with information on how to spot and deal with informers, infiltrators, and provocateurs in our ranks.

Who is an Informer?

There are actually two kinds of informers. The deliberate informer is an undercover agent on the payroll of government or industry. The second type is the activist-turned-informer. Both kinds try to infiltrate our ranks and are equally dangerous to our movements.

Most activists will be intimately familiar with their local police forces. Be aware that cops do not only show up in blue uniforms — but routinely practice crowd infiltration and carry out surveillance and investigative activities either alone or jointly with the RCMP depending on the type of case. Watch for them on demonstrations — as they like to come along and take photographs and video for the record — and they often appear in crowds as “fellow demonstrators.”

The Counter-Insurgency Model

Most Western nation-states follow a model of counter-insurgency developed by a British intelligence expert named Kitson who wrote, *Low Intensity Operations*, after much field work in the colonies. He broke down movement development into three stages:

The Preparatory Phase: is when the movement is small, tends to focus on education, publishing and groundwork.

The Non-Violent Phase: is when the movement takes on more of a mass character. Large demonstrations are the norm.

In the Insurgency Phase: the movement has taken on a popular character. Perhaps a more assertive, guerrilla component has emerged.

Kitson advises that the primary work of the intelligence agency should occur during the preparatory phase. At this time the movements are most vulnerable. They have not experienced a high degree of repression. They consider talk of security as mere paranoia. As they are not breaking laws they believe that it is safe to organize completely openly. The intelligence agency is therefore able to exploit these conditions and develop detailed dossiers on a wide range of people. The information will be extremely valuable to them later on.

Important historical revolutionary activities and groups began as small, serious-minded projects that grew in spite of surveillance and repression. It is therefore important to

of domestic intelligence in Canada. In this way, we can better understand how to avoid its traps.

An Overview of Domestic Intelligence Organizations

The Canadian Security and Intelligence Service (CSIS) is probably the best known of the “security” agencies that deal with activist “threats.” Its predecessor was the Security Service division of the Royal Canadian Mounted Police, (RCMP-SS). In 1984, following the MacDonald Commission on the illegal activities of the RCMP, the civilian spy agency CSIS took over RCMP spy work. That said, the RCMP did not abandon its intelligence gathering, it’s just that CSIS specifically gathers political intelligence.

The split from the RCMP allowed the new spy agency to do legally what the Mounties had been doing illegally. At the operations level, the new agency was granted more leeway in terms of public accountability than the Mounties had ever had.

CSIS carries out a wide range of surveillance activities. Since they are not a law-enforcement agency and since their evidence is not used in court, nothing stops them from contravening the few regulations that do exist regarding privacy rights. For example, CSIS is not required to inform people, as is RCMP, ninety days after a wiretap (or bugging) is over.

Agents working for CSIS are allowed, with “authorization,” to enter people’s homes to plant bugs, wiretap phones, open mail and look into health, employment and government records without ever having to tell a targeted individual what they are doing. The information that they gather is used to build profiles and dossiers (files) on individuals, organizations, networks, etc. This information is also passed on to other wings of the federal security system who are responsible for “law-enforcement,” and will then obtain whatever warrants

are necessary for legal surveillance (to be brought into court as evidence).

The National Security Investigation Service (NSIS) is the primary law-enforcement wing in Canada. The NSIS is a section of the Royal Canadian Mounted Police (RCMP). Most major cities across the country have an NSIS office including Vancouver, Edmonton, Montreal, Ottawa, and Toronto. The NSIS maintains a computer database on activists, immigrants and so called “terrorists” which is housed in Ottawa.

It is believed that the Vancouver NSIS employs between 12 and 18 members. Within NSIS there are several sub-groups called Team 1, Team 2, Team 3 — etc. that have different investigative targets.

They employ informants, infiltrators, personal physical surveillance, electronic surveillance including phone and room “bugs” and other means of investigation and research.

The RCMP/NSIS also have other resources at their disposal during counter-insurgency operations. “Special O” is a team of surveillance specialists that may be called upon. “Special I” is a penetration team whose specialty is to break into homes, vehicles and other properties for investigative purposes. They are the team, which among other things, installs listening devices, photographs building interiors, etc.

In a long-running case based in Vancouver, all of these methods of surveillance were used against several Vancouver activists. During the Vancouver investigation, house and vehicle bugs were located by some targeted individuals. The bugs had large battery packs attached to facilitate less frequent battery changes. The NSIS also visited several activists across Canada in an attempt to question them regarding the individuals under investigation.

The Golden Rule of Silence

It needs to be stressed throughout our movements that no one is under any legal obligation to provide to the police anymore information than one’s own name, address and birth date, and this only if one is under arrest. That is it! Saying anything more jeopardizes security. Even answering seemingly insignificant questions can assist the police in developing personality profiles on a range of activists. It may not be “evidence” but it is used to give police “leads” on other suspects and construct intent during legal proceedings. The only principled response to police questioning when under arrest is to say nothing more than your name, birth date and address. If questioned further you can simply say “I have nothing to say (except in the presence of my lawyer.”

The Communications Security Establishment (CSE) is an agency of the National Defence / War department, which has been long clouded in secrecy.

They collect and process telephone, fax and computer communications of foreign states, corporations and individuals. The federal government uses the intelligence gleaned from the data to support troops abroad, catch “terrorists” and “further Canada’s economic goals” (what that means is up to them).

Although the CSE is not technically allowed to collect the communications of Canadian citizens, it is known to be a partner in the Echelon project — a multinational monitoring operation which sees CSE and counterpart agencies in the United States, Britain, Australia and New Zealand share intercepted communications of interest with one another, effectively creating a global surveillance web.

The Terrorist Extremist Section (TES Unit) is British Columbia’s anti-terrorist unit. A joint Vancouver/Victoria Police Department/RCMP unit called the Organized Crime Agency (formerly the Coordinated Law Enforcement Unit — CLEU), it is believed that the this unit employs two or three members only.