Security Culture: a handbook for activists

This handbook is the first edition of what we hope will be an evolving and growing document dealing with security issues and canadian activism.

A lot of this information is general and can be applied to any locality - other information is easily adapted to fit other situations.

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

Second edition - prepared August 2000

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

The other type of activist-informer is person who cracks under pressure and starts talking to save his/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.

We have to know the possible consequences of every action we take and be prepared to deal with them. Someone who is easily influenced by his/her parents or dependent on them for support is not a good candidate for actions as they can be persuaded too easily to cooperate with the authorities. There is no shame in not being able to do an action because of responsibilities that make it impossible to do jail time. If others are depending on you for support or you aren't willing to lose your job or drop out of school, DON'T DO THE ACTION.

Make certain that others in your affinity group are not in situations which may cause them to cooperate with the police or abandon their friends.

Some things to look out for in people you choose to do illegal direct action with are lengthy criminal records and drug addictions which can often be used by the police to pressure activists into giving them information. Two activists were recently put in jail in Canada because a third party panicked - mainly about not being able to get his drugs in jail - and talked to free himself. (This is not to condemn those who have drug habits or criminal records - but are certainly things to keep in mind).

Don't be afraid to talk about this. Ask hard questions, and if you aren't convinced that someone will be able to stay strong if the worst happens, then designate that person to do support. Make sure that those who go into battle with you are willing and able to take whatever comes, even if it means giving up their freedom for your goals.

Remember - there is no excuse for turning in action 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 far-reaching and can have devastating effects.

questions about the direct action groups, individuals and illegal activities. S/he will suggest targets and volunteer to do reconnaissance as well as take part in the action.

An example of infiltration tactics can be found in an incident that occured a few years ago when U.S. Surgical hired a security firm to infiltrate Friends of Animals in Connecticut. Their operative convinced an activist to put a pipe bomb in the car of the president of U.S. Surgical. Needless to say, the police were waiting for her and she ended up being charged with attempted murder.

State and industry infiltrators have been identified in operation in British Columbia over the past few years - attempting to incite illegal activity, sowing disruption in action camps, and gathering information on the who, what and when of our movement's activities

Everyone who asks a lot of questions about the direct action isn't necessarily an infiltrator, but they ARE the ones to watch (at the very least, we should be educating them about security culture). Explain to new activists that direct action tactics can be risky (though some risks are worth taking!) and that it is dangerous to ask a lot of questions about it. If the person persists in asking questions, STAY AWAY FROM THEM!

Any activist who can't understand the need for security is someone that should be held at arm's length from the movement.

Placing infiltrators into social justice movements isn't anything new. It was done to the Black Panthers and the peace movement in a big way. Unless you are only working with people you've known for years and who have earned your trust, you should assume there is an informant in your midst and act accordingly.

This doesn't mean that no one else should ever be allowed into the "inner circle." On the contrary, if our movement is to continue to grow, we must always be recruiting new members; we just need to keep security uppermost in our minds and exercise caution at all times.

Possibly an even greater threat 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 s/he's done, make sure this person never has any knowledge that can incriminate you, because sooner or later, the wrong person will hear of it. These activists don't mean to do harm, but the results of their bragging can be serious.

Introduction:

Resistance has been on the rise for the past few years, with activists adopting more and more effective tactics for fighting back. Now, more than ever, we pose some threat to the status quo. Our increased activity and effectiveness has meant that the RCMP, FBI, and local police have continued to escalate their activities against us. 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 (and even US) activist who is interested in creating and maintaining security awareness and culture in the radical movements. It is not nearly complete - but is what we have got finished at the moment. 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.

If this material appears familiar to you - its because this is the second edition of this zine that we have put out... mostly to correct spelling errors and other small things. The three articles in this pamphlet have been mostly cobbled together from other writings that already exist on this subject out there so we don't claim any of this to be 100% original material - though we have included quite a bit of fresh info on the Canadian state and its operation (mostly because we have found the majority of info out there to be very focussed on US law enforcement). We hope that you will put the material contained within to good use!

everything you ever wanted to know about informers and infiltrators

[redacted] [redacted] [redacted]

Informants and infiltrators operate in every radical movement. The rise of militant radicalism as seen at the WTO protests in Seattle, and the declarations by activists to continue the struggle in the streets and underground - mean that more and more attention will be paid to activists by law enforcement. Part of this will mean sending more infiltrators amongst our ranks to bribe and entice those weak individuals already involved.

Non-violent movements need to learn to identify such people and and let them know that their actions will never be tolerated by activists in any way.

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

Who is an informer?

There are actually two kinds of informers. The deliberate informer is someone who infiltrates an organization with the specific intent of getting incriminating evidence against activists or even setting them up to be arrested. These infiltrators are either on the payroll of a government agency or may be hired by industry. The second type of informer is the activist-turned-informant--either unwittingly or because of pressure put on them by the authorities. Make no mistake, both kinds exist throughout our ranks and are equally dangerous.

Let's discuss the deliberate informer (infiltrator) first. They are often difficult to identify, they come in all ages and types, but they usually have a similar modus operandi--they come out of nowhere and all of a sudden, they are everywhere. Whether it's a meeting, a protest, or an action, this person will be right in the thick of it.

Keep in mind however that this is also the hallmark of a new activist, whose enthusiasm and commitment is so strong that s/he wants to fight the power every minute of the day.

How to tell them apart? Well, a planted infiltrator will ask a lot of

Security Culture

What it is, why we need it and how we implement it...

Agitators; liberationists; abolitionists; union organizers; revolutionaries... From large uprisings challenging the entire political structure, to isolated environmental and social struggles, people have always worked to create a better world. For government the response has usually been to jail activists and revolutionaries through use of the courts and police forces.

As direct action movements become more effective, government surveillance and harassment will increase. To minimize the destructiveness of this political repression, it is imperative that we create a security culture within our movements.

This pamphlet is essential reading for anyone who is associated with groups that advocate and/or utilize sabotage, theft, arson and more militant tactics. The advice herein also applies to anyone who is associated with groups that practice civil disobedience, especially since membership often overlaps and gossip travels freely between groups.

Even if you have never picked up a monkeywrench or been arrested for civil disobedience, even if you think you have nothing to hide, these guidelines will enhance your personal safety as well as the movement's overall effective-ness. Surveillance has been set up on all sections of political movements in the past.

Governments in the western industrialized world have targeted groups that have advocated sabotage and groups that have not, movements that have been militant and movements that have been markedly pacificst. The government's security machinery serves political and economic objectives, and there are over 250 political prisoners in Canada and the US that can testify to this from firsthand experience. By adopting a security culture, we can defeat various counterintelligence operations that would otherwise disrupt both mainstream organizing and underground resistance.

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.

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 undergound 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 wrong to speak about a specific 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.

Please note: this is not to say that it is wrong to speak about direct action in general terms. It is perfectly legal, secure and desirable that people speak out in support of mokeywrenching 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 specifically about actions and involvements.

The first situation would be if you were planning an action with other members of your small group (your "cell" or "affinity group"). However, you should never discuss these things 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.

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.

It is important that as a movement in we need to learn to practice security at all points in the movement's development. Remember that the State is interested in knowing about activists' beliefs, not just in "hard evidence". Learn and practice security to protect ourselves and our peoples. Don't be afraid. Remember - If an agent comes knockin', do no talkin'.

gleaned from the data to support troops abroad, catch "terrorists" and "further Canada's economic goals" (and 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.

Most activists will be initimately 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

The second exception occures after an activist has been arrested and brought to trial. If she is found guilty, this activist can freely speak of the actions for which she was convicted. However, she 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 in other publications.

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 quite obvious: if people don't know anything, they can't talk about it. It also means that only the people who know the secret can also face jail time if the secret gets out. 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 selfish desires in-check so we do not

jeopardize the safety of other activists or ourselves. People who place their desire 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 movement solidarity and trust.

Gossiping: Some weak characters 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 a grand jury or other investigation.

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 as the people who he told (they can become accessories after the fact). An activist who brags also sets a horrible example to other activists.

I**ndirect-Bragging:** Indirect-braggers 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 (that kind of lying is acceptable).

EDUCATE TO LIBERATE

It is fairly easy to spot those activists who compromise our movement's security. So what do we do with people who exhibit these behaviours? Do we excommunicate them from our movement? Actually, no--at least, not for a first offense.

The unfortunate truth is there are numerous 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 be educated. Even seasoned activists can 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

of domestic security. The NSIS is a section of the Royal Canadian Mounted Police (RCMP). Most cities across Canada 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.

It cannot be stressed enough that no one is under any legal obligation to provide the police with any information other than one's own name and address. That is it. Saying anything more jeopardizes individuals' and movement security. Even answering seemingly insignificant questions can assist the police in developing personality profiles on a range of activists which may not contain "evidence" but may instead be used to give police "leads" on other suspects and to construct intent during legal proceedings. The only principled response to police questioning is to say nothing more than name and address.

The Communications Security Establishment is an agency of the defence 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

of our growing movements. One of the key aims of COINTEL-PRO operations against the Black Panthers and American Indian Movement was to spread paranoia and distrust among those freedom fighters so that they would find it hard to accept new people into their work.

It **is** possible to build a movement large and at the same time create security culture. Arming ourselves with knowledge about how the system works against activists is the first step to creating that culture. The central aim of this article is to give a brief run-down of how domestic intelligence works in Canada so that 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". They were originally a special surveillance wing of the RCMP until 1983 when they were split off into a separate agency due to protests that they were acting as a secret organization that was contravening Canadians' democratic rights to organize. Essentially, 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 freedom and more leeway than the Mounties ever had.

Today they continue to carry out a wide range of surveillance. As they are not a law-enforcement agency and therefore their evidence is not used in court, there is nothing stopping them from contravening the few regulations that exist regarding privacy rights. For example, CSIS is not required to inform people, as the RCMP does, ninety days after they have been wiretapped or bugged.

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. The information that they gather is often 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

help. We must NEVER let a breach in security occur without acting to correct it. If an acquaintance of yours 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 educate this person in a manner that encourages him to listen and to change his behaviour. It should be done without damaging his pride. You should be humble and sincerely interested in helping him to become a better person and a more effective activists. Do not maintain a "holier than-thou" attitude. This will inevitably raise his defenses and prevent him from absorbing or using any of the advice you offer. Remember, the goal of educating people is to change their behavior, not boost your ego by showing them how much more security-conscious you are.

If possible the educational session should be done in private, so the person does not have to contend with the potential ‘pride’ issues. The educational reprimand should also be done as soon as possible after the mistake to increase its effectiveness.

If each of us takes on the responsibility of educating those who slip up, we can dramatically improve movement security. Once people recognize lying, gossiping, bragging, and indirect-bragging as the damaging behaviours that they are, they will soon end. When we develop a culture where all breaches of security result in an immediate reprimand, all sincere activists will quickly get with the program.

DEALING WITH CHRONIC SECURITY PROBLEMS

So what do we do with activists who repeatedly violate security precautions even after multiple educational sessions? It's unfortunate, but the best thing to do with these people is cut them loose and kick them out of our meetings, basecamps and organizations. With law enforcement budgets on the increase 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 defense against informers and agents who try to infiltrate groups. Imagine an informer who, every time she asked another activist about that person’s activity , received a reprimand and an education on security. That informer would get frustrated really easily. Once the activists discovered she continued to violate security precautions after being repeatedly educated, they would have grounds for her dismissal. And that would be one less informer for us to deal with!

a brief primer on the canadian state security apparatus

Recent repression against activists in British Columbia illuminates the need for grassroots people to understand and practice movement security. Police monitoring, infiltration and agent provocateurs are all techniques used by the state routinely against activists to turn up information about the activities of our movements and ourselves.

Although many activists have trouble believing that state security agencies have that much interest in their affairs, a few key court cases and hearings have helped activists to gain access to information that proves that police spying on activists is routine in Canada.

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, and local activists have been targeted by provocateurs who have tried to convince them not only to disclose information but to break the law.

The Canadian security apparatus has identified a number of our movements as threatening to national security. They have targeted people and organizations widely. Even avowed pacifists have been included in surveillance and repressive measures. According to Canadian Security Intelligence Service (CSIS) annual reports of the past five years, the Native Resistance and the Environmental/Animal Rights movements have been primary targets.

With the rise in militant First Nations struggles, covert direct action against corporations, and the growing focus by the media on general "anarchist" politics due to events in Seattle around the WTO among other major increases in movement strength and militancy, we can be pretty sure that this has been marked by a growing level of surveillance and monitoring as well.

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