Introduction to Security Culture

originally borrowed from resist.ca
mirrored from C4SS

The first step in recognizing security risks in a community is working towards creating a security culture. Below we have compiled some relevant materials and links that should be used in conducting security workshops and educating activists that you work with.

As our direct action movement becomes more effective, government harassment will only increase. To minimize the destructiveness of this government harassment, it is imperative that we create a "security culture" within our movement. Violations of security culture include behavior is inappropriate because it intensifies government harassment, jeopardizes the freedom of other activists, and destroys the trust within the movement.

COMMUNITY ORGANIZING AND STATE REPRESSION

It was not that long ago that discussions about security culture were seen as not relevant to the vast majority of community organizers. As long as one didn't "break the law" it was assumed that social freedoms in North America and Europe would allow for the expression of dissent without a rise in repression. A number of events have conspired since the late nineties to change the landscape of organizing considerably.

New legislation – the PATRIOT Act in the US and Bill C-36 in Canada – which have been sold to the public as required to fight the spectre of terrorism in a post-911 world, serve double-duty in giving the state new laws with which to crack down on internal dissent. A rise in state-hyped racist hysteria, has made community organizers from middle eastern origins (or other "suspicious" backgrounds), increasingly targets of incarceration without cause, and other abuse at the hands of governments eager to deflect attention from the real issues of failing economies and unpopular wars. In many countries, governments have enacted laws to make it illegal to work with overseas organizations now declared "terrorist" – putting at risk communities who have worked to support liberation fighters around the world.

It follows that those who fight to change the world will be met with resistance by those who do not want it changed. One does not have to participate in extralegal activities to raise the interest of state security forces (whether those be local, regional or national agencies). Security culture must no longer be thought of as merely the domain of those who might break unjust laws – but as something that is part of the organizing toolbox as a mechanism for community self-defense.

The guidelines presented here are designed to enhance your personal safety as well as the overall effectiveness of our movements. By adopting a security culture, we can limit or neutralize counterintelligence operations meant to disrupt our political organizing, be it mainstream or underground.

TOWARDS AN EXPANDED DEFINITION OF SECURITY CULTURE

Creating secure communities is about more than being educated about the state and its security forces. Fundamentally, it means creating working dynamics of respect, education and inclusion in all our work. Building strong communities that act in solidarity with one another is the best protection against infiltration, disruption and other conditions of repression.

So what is a security culture? It's a culture where the people know their rights and, more importantly, assert them in all situations. Those who belong to a security culture also know what behaviour compromises security and are quick to work with people who exhibit insecure or oppressive behaviour. Security consciousness becomes a culture when a community as a whole adopts this awareness and demonstrates that those behaviours which violate security are unacceptable.

SECURITY CULTURE MEANS CHALLENGING OPPRESSION

Security culture is about more than just targeting 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 oppressive practices aren't feeding into intelligence operations being carried out against our community.

Within the histories of groups targeted by COINTELPRO (such as AIM and the BPP), and certainly within the animal rights and environmental movements, there are many example of how oppressive behaviours created conditions ripe for FBI manipulation.

Underlying sexism in some groups has meant that women trying to raise security concerns are not taken seriously, or (on the other end), are not suspected as informers simply because they are women. A tokenistic approach to recruitment has lead socialist organizations to bring in new members who fit their 'ideal' of what the working class should be – only have them to later turn out working for the British Home Office.

Racism, sexism and homophobia in the movement spread division that create overall weaknesses and create openings easily manipulatable by state operatives. Exclusion can make those people who feel marginalized by group practices more open to infiltrators.

Obviously, our movements still have a lot of work to do before we have satisfactorily addressed issues of oppression – but what is important here is a recognition that oppressive behaviours feed into poor community security.

(IN)SECURE PRACTICES

The following section was originally written for an audience engaged, or on the periphery of extralegal activity, and so focuses on "underground" groups. We would like to add that the same rules apply to discussions about individuals involved in or providing support groups considered "terrorist" by western governments (but who are in actual fact, liberation fighters at odds with US foreign policy). It is generally good practice to limit discussion about movement individuals where you are unsure what information about them is "public" knowledge.

As community organizers, a lot of activists like to verbally engage with each other and have no trouble spending hours discussing theory, tactics, and strategy. This is an essential part of building our analysis and work, but in some cases this can put ourselves or others in jeopardy.

WHAT NOT TO SAY

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

- your own 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 own or someone else's participation 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, or with activities that may raise the interest of the state (such as advocacy of certain groups or tactics). These are unacceptable topics of discussion regardless of whether they are rumor, speculation or personal knowledge.

Please note: this is not to say that it is incorrect to speak about direct action in general terms – just be sure that you don't link individual activists to specific actions or groups. It is perfectly legal, secure and desirable that people speak out in support of all forms of resistance (though if you're involved with illegal activity, it is probably best that you don't openly advocate for breaking the law as that alone can raise state interest in your life).

THREE EXCEPTIONS

There are only three times that it is acceptable to speak about specific actions that may be against the law. These are the only situations when it is appropriate to speak about your own or someone else's involvement or intent to commit an illegal act.

The first situation would be if you were planning an action with other members of your small group (your "cell" or "affinity group"). These discussions should never take place over the Internet (e-mail), 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 carefully and without compromising security. Advice on secure communication techniques can be found at elsewhere on this site.

BOTTOM LINE SECURITY

If you are engaged in activity that is considered illegal, it is best to take a lesson from veteran activists of the direct action movements and only allow a select few to know about your activity. Those few people should consist of only the individuals who you are doing work and actions with and 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 breaches 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 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.
- **Gossip & Rumors**: 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. New anti-terrorist law in both Canada and the United States allows state security forces to carry out raids on individuals based on nothing more than hearsay evidence.

- **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.
- **Indirect-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 . Concealing sensitive information from even trusted comrades is far better than jeopardizing underground work.

SELF-EDUCATION TOWARDS LIBERATION

With the above information about security, it should be easier to spot those activists who compromise our movement's security. So what do we do with people who display these behaviours? Do we shun or expel them from our groups and projects? Actually, no – not for the first security violation, at least.

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 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 a superior, "holier than-thou" attitude. Such an attitude can raise an individual's defenses 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 recognize that lying, gossiping, bragging, and inappropriate debriefing damages both themselves and others, these behaviours will soon end. 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 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 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!

ADOPT A SECURITY CULTURE NOW!

Activists are restless and resistance is on the rise. Some people are adopting radical and confrontational tactics. The more we organize and are effective, the more police forces continue to escalate their activities against us. For direct action movements to continue, we need to consider our security more seriously. Good security should be made one of our strengths.