Security Culture Guidelines

Rising Tide Vancouver, Coast Salish Territories
January 2015

With increasing evidence of government and corporate surveillance of Environmental and Indigenous groups, Rising Tide Vancouver, Coast Salish Territories (RT-VCST) operates on the assumption that meeting spaces, telephone and online communications, and even closed action planning meetings are vulnerable to infiltration and electronic surveillance. By carefully thinking about our communication we can counter some of this surveillance.

Grassroots surveillance (hacking), has revealed Big Oil's plan to discredit and isolate RT and other 'radical' climate justice groups, using age-old techniques like divide and conquer. We can act to counter that too. Rather than become paranoid, we strive to develop a healthy 'security culture' which allows us to organize effectively while maximising our, and others, safety. We consider being supportive and welcoming part of an effective security culture, as is developing ways to deal with abusive and disruptive behaviour.

Some of the guidelines below may feel strange at first but don't worry, it's called security 'culture' because it eventually becomes instinctive. And the more people who follow the guidelines, the less likely it is that any one person will put themselves or others in danger.

Guidelines we try to stick to (acknowledging that they are a work in progress):

1. Consider the Nature of the Group

RT-VCST is an above ground organization, and is affiliated to other RT groups in the Rising Tide North America (RTNA) network. An important part of security culture is understanding that above ground organizations like RT-VCST are relatively easy to infiltrate, and some activities are therefore not strategic in such groups. *Please read the RTNA Principles for some f*ood *for thought on the nature of Rising Tide* –http://risingtidenorthamerica.org/features/principles/

2. Understand Norms of Behaviour as Part of Security Culture
Building a collective and movement you feel good about is part of good security culture:

"One of the most effective ways to counter surveillance and harassment is to have people remain committed to activism for years [by building a] group (and activist community) that people enjoy being a part of. Another positive approach to the problem of infiltration is to focus on eliminating bad behavior." Ruckus Society, p7.

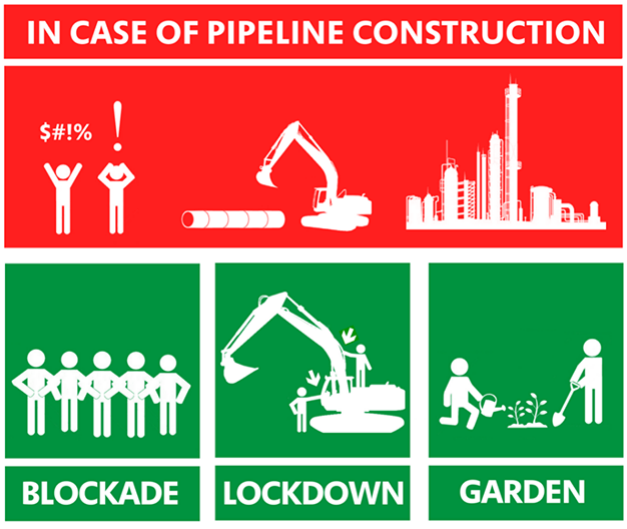
'Bad behavior', such as false accusations (and other ways of creating divisions) within or between groups, is so destructive that it is one of the favored tactics of paid infiltrators in the role of 'Agents of Chaos'.

"Political groups often worry about infiltrators and informers. Divide and Conquer is one of the primary ploys used by infiltrators. Everyone who practices Divide and Conquer is not an agent – but a group that develops strategies to guard against this dynamic will also protect itself from some of the damage potentially caused by infiltrators" Starhawk, p224.[1]

Infiltration (state and industry) does happen, but paranoia about infiltration can be even more damaging. Norms of respectful behaviour are essential to good security culture.

3. Open or Closed?
When we plan an action, we decide at the beginning how open that action and it's planning will be, we then adjust our organizing accordingly. If we are organizing an action which is intended to bring out thousands of people, and we're inviting them online, it is an open action. The cops will know where the action is happening and this information does not need to be kept secret.

If, however, we are organizing a small non-public action where we are going to arrive unexpected at a company's head office for example, the element of surprise is key; this is therefore a closed action, with tighter security. Some actions have elements of both – an open action that is publicised with a surprise target which is closed.



Need to Know With closed actions we operate on the idea that only the people involved in the action need to know the specifics of it (specifics such as the target, means of entry, exact timings, etc.) The more people who know, the more it puts the action and those involved at risk. By

[1] (2011) *The Empowerment Manual: A guide for collaborative groups.* New Society Publishers

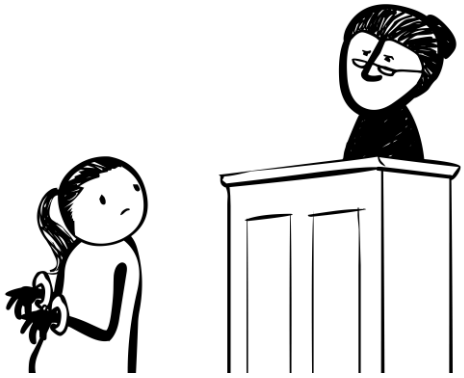
telling someone else about the action, who does not need to know, you are putting that person in a vulnerable position where they may be legally implicated later.

We acknowledge that this can be very tricky within a collective that uses consensus, so that is why we strive to agree on security levels at the beginning, and only communicate what the collective needs to know. However, the collective must be involved in deciding on the types and character of Rising Tide actions. Actions that fall clearly within bounds supported by the collective can be carried out by RT sub-committees without discussing the exact timing or targets with the collective. It is a hard balance and we are leaning as we progress.

4. Think about what you say and type

Consider observation from police and hostile media. Imagine what you post on the Rising Tide website or Facebook page ending up being used in the media to justify police violence or search warrants. Also, police do read emails and bug phones; think about how your communication impacts group – and action – security.

Something said as a joke can sound very different when introduced as evidence in court, and then repeated in the mainstream media. Remember that at the Toronto G20 trial "stupid jokes and bragging" were used in court[2]. Get into the mindset that anything you say in a meeting or over the phone, or type, post or research online could be read out in court.



5. Get Used to Speaking Generally

It can feel safe after an action has passed to tell people about specific details (how something was accomplished, who did what, etc.). Please don't. It can feel cool to know other people who are interested in doing badass things; don't talk about them as it puts them at risk. You can talk about how things are done, so others can learn from experience, without specifying specific actions or people.

6. Don't Ask, Don't Tell

Just as we keep specifics of some of our own actions to ourselves, we don't inquire about confidential information from other people or groups. If someone is asking you something you don't feel comfortable sharing, don't answer.

[2] Toronto G20 Main Conspiracy Group: The Charges and How They Came to Be (2nd Edition 2012) http://zinelibrary.info/files/torontoconspiracy.pdf p18.

7. Don't Talk to Cops (when they want to talk to you)
Cops normally only talk to you when they want to get information from you, intimidate you, or spread misinformation. That information might be used against you, and/or others in the group. The easiest thing to do is to not engage with them. If they have not detained or arrested you, you are free to leave. If they have detained you, all you have to tell them is your name, address and date of birth, then you have the right to ask for a lawyer. Tell them anything more and it jeopardizes security.

One exception is where groups decide on a place and time to talk in mass to the police, military, or other individuals 'on the other side' about the ethical reasons for an action. This is a tactic that requires group discussion, and preferably training in advance.

8. Consider Your Own Situation
Know the likely consequences of your actions. Think about your limits and your situation. If you are not 'arrestable' – for reasons like work, visa status, life circumstances – don't place yourself in that position, the cops may use this to put pressure on you for information once arrested. Thinking about this in advance will enable you to interact with police far better if you are arrested, in turn this will keep you and others safer.

9. Build Community
Getting to know the people you organize with (their friends, family and social circles, what they get up to - work, school, hobbies, etc.) not only mitigates paranoia but also helps us to build a supportive community. Building these friendships can also energize us to stay involved and continue organizing amid the security state.

10. Get Active, Not Paranoid
Paranoid means being "so suspicious of others that you are incapable of doing what you need to do" (Ruckus, p7). Paranoia is debilitating, avoid the trap; get active, have fun, just be careful and consciously think about what you say and type before you do it.

More reading:
Security Culture for Activists - Ruckus Society
www.ruckus.org/downloads/RuckusSecurityCultureForActivists.pdf

Security Culture – a handbook for Activists
www.sproutdistro.com/catalog/zines/security/security-culture-a-handbook/

Toronto G20 Main Conspiracy Group: The Charges and How They Came to Be (2nd Edition 2012) http://zinelibrary.info/files/torontoconspiracy.pdf