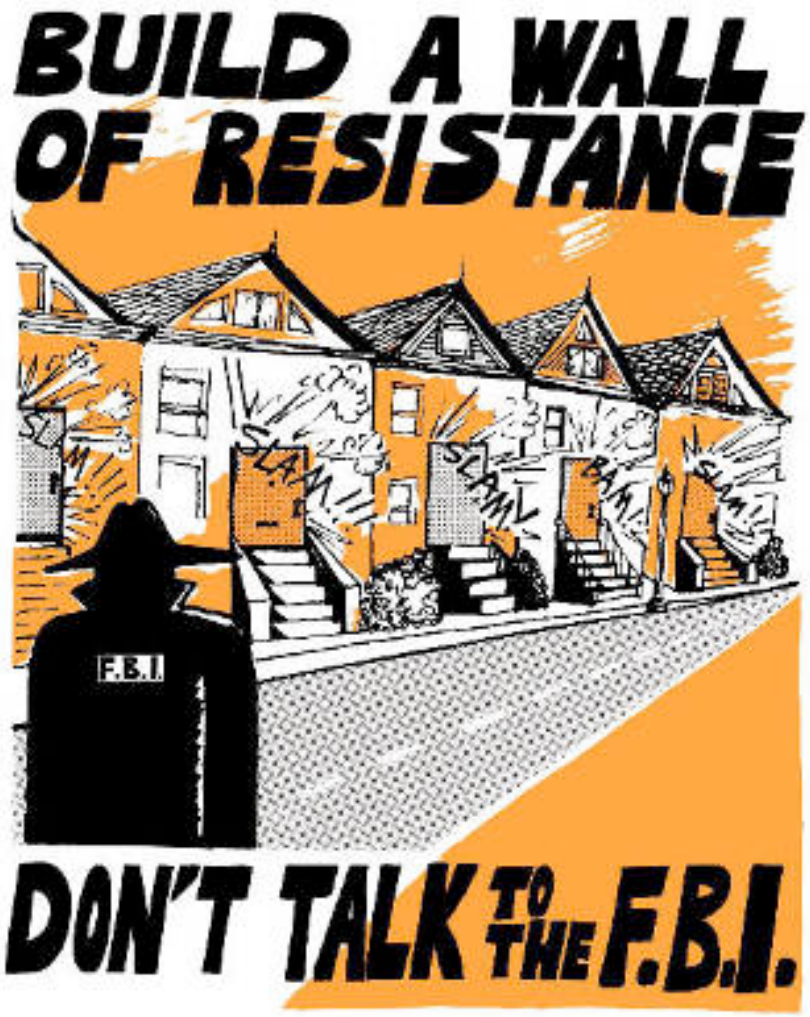
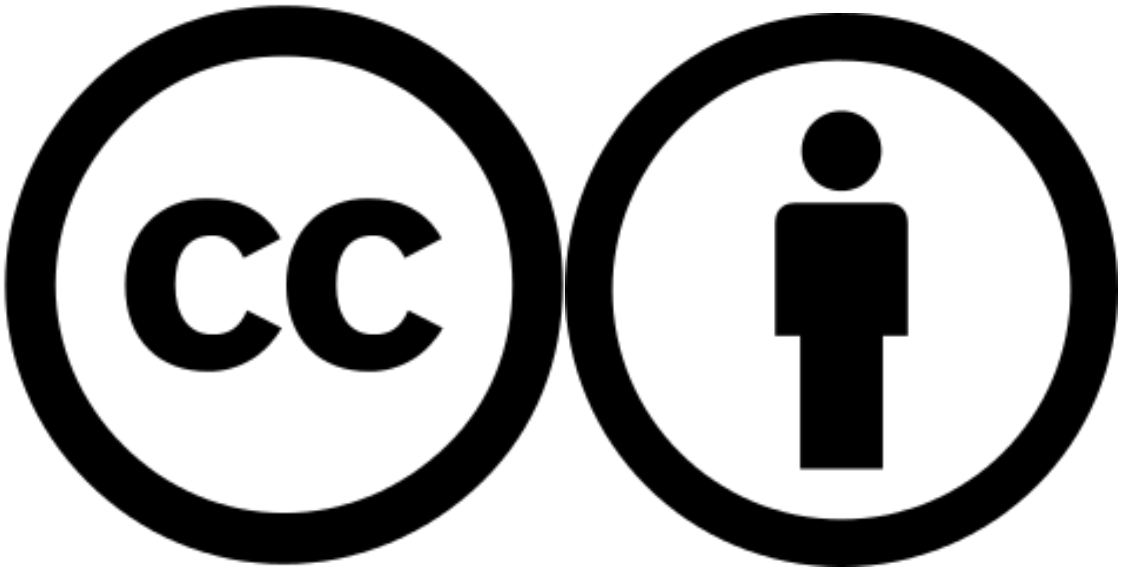
Security Culture: A Beginner's Guide

By Deep Green Resistance

Edited by Kyle Rearden





Editor's Foreword

This guide on security culture focuses more on how to more effectively organize affinity groups rather than on digital security or implementing any grey man principles. Emphasis lies in vetting and ostracism, and how to do so as diplomatically as possible. Keeping one's counsel appears to be the primary tactic used to avoid and deter surreptitious police interrogations.

Care has been taken to reproduce *Deep Green Resistance*'s webpage on security culture. Formatting has been made in order to facilitate easier reading and printing. This has been undertaken with *DGR*'s explicit permission.

If anything, it would seem that leaderless resistance is preferably to formal organizations that can be infiltrated, subverted, and broken apart. As long as individuals take their liberty of free association seriously, then it will be a lot easier for American political dissidents of all stripes and flavors to keep their own houses clean, so to speak, of hostile elements intent on disrupting their attempts to secure their Liberty.

Kyle Rearden
Austin, Texas
June, 2015

The bare truth is that we live in a surveillance state that is unparalleled. Many people are legitimately worried or afraid of state repression. But this fear can become paranoia and paralysis. As a result, some will not get involved in radical activism. Others will stay involved, but their paranoia will create a stifling atmosphere and drive people away. The result? Our movements die.

Security Culture – a simple set of rules anyone can follow – reduces paranoia and fear, and makes us safer so that we can do our work effectively. This page is a basic introduction to security culture and should not be considered comprehensive. Be smart and adapt to your specific situation.

What is Security Culture?

Security culture is a set of practices and attitudes designed to increase the safety of political communities. These guidelines are created based on recent and historic state repression, and help to reduce paranoia and increase effectiveness.

Rules of Security Culture

Don't Talk About…

- Your involvement or someone else's involvement with an underground group.
- Your or someone else's desire to get involved with such a group.
- Your or someone else's participation in illegal action.
- Someone else's advocacy for such actions.
- Your or someone else's plans for a future illegal action.
- Don't ask others if they are a member of an underground group.
- Don't talk about illegal actions in terms of specific times, people, places, etc.

Nonviolent civil disobedience is illegal, but can sometimes be discussed openly. In general, the specifics of nonviolent civil disobedience should be discussed only with people who will be involved in the action or those doing support work for them.

It's still acceptable (even encouraged) to speak out generally in support of monkeywrenching and all forms of resistance as long as you don't mention specific places, people, times, etc., but only if this is legal in your own jurisdiction. Even if voicing support for monkeywrenching is legal in your area, be aware of possible repression or consequences so you can make an informed decision about what level of risk you would be comfortable with.

Never talk to police officers, FBI agents, etc.

- It doesn't matter whether you are guilty or innocent. It doesn't matter how smart you are. *Never* talk to police officers, FBI agents, Homeland Security, etc. It doesn't matter if you believe you are telling police officers what they already know. It doesn't matter if you just chit chat with police officers. Any talking to police officers, FBI agents, etc. will almost certainly harm you or others.
- If you talk to a police officer, you give him or her the opportunity to testify against you based on what you said or what they say you said.
- Simply and politely say you wish to remain silent. Ask if you are being detained or are under arrest. If you are not, then walk away. If you are arrested or detained, repeat to everyone who asks you that you wish to remain silent and that you wish to speak to a lawyer. Say nothing else but your name, address, and birth date.
- Most convictions, whether people are guilty or not, come from people talking, not from investigative work.
- Don't snitch. A snitch is someone who provides information to the police or feds in order to obtain lenient treatment for themselves. Often, snitches provide information over an extended period of time to the police. Sometimes this occurs after they are arrested and asked to become informants. In return, they may receive money or have their own illegal behavior ignored by the police. Learn more about one prominent snitch.
- Learn about interrogation tricks and threats.
- Watch Don't Talk to Cops – Part I and Don't Talk to Cops – Part II on YouTube.

Never allow a police officer, FBI agent, etc. into your home if they don't have a search warrant

- If you invite a police officer into your home, they have consent to search your home.
- If they come to your house to ask questions, do not let them in. From inside your door, or from outside with your door shut behind you, politely say "I wish to remain silent." Ask them if you are under arrest or if they have a search warrant. If they say no, go back inside your house and close your door politely. If they come in anyway, don't resist arrest. Say "I do not consent to a search." Take note of who they are and what they do.

Be Smart

- Learn the laws in your country/state/jurisdiction: learn what you can and can't say; learn what acts are legal and illegal; learn what previous activists have been tried for and what is permitted legally.
- Find out the details of activist and protest lawyers/legal advocates in your area: if you go on an action, make sure you write their telephone number on your body in a permanent marker.

- Link in with experienced activists: they will have a wealth of experience and knowledge about the landscape of activism where you are, and can teach you what are the local logistics and strategies for staying safe.

Myths of Security Culture

Myth # 1

"Hiding my identity aboveground makes me safe."
"If I read the DGR website I will be on a government list."
"I don't want my name on a registration list for a DGR workshop so they won't know who I am."

- Any action involves risk. Nothing can guarantee safety. Any effective aboveground action can lead to repression. Security culture makes us more effective.
- Aboveground movements protect themselves almost exclusively through numbers and public solidarity.
- There is no way to effectively do aboveground work and keep your identity hidden. Nor is it beneficial or necessary to hide your identity to do aboveground work.
- Aboveground movements can only build numbers and public solidarity by being public, open, and expressing support of the movement in order to attract others.
- Operate on the assumption that all internet and phone communication is monitored. However, since aboveground movements have nothing to hide, except occasional nonviolent civil disobedience, we must use the internet and phones to communicate in order to be able to organize effectively.
- One of the main roles of the aboveground is to be the public face of the movement. We stand publicly and say "I support this strategy and I advocate for DGR," for example. This important work cannot be done if we are constantly trying to hide our identities.
- There are perfectly legitimate reasons for wanting to keep a low profile, but hiding your identity completely while engaging with any movement is practically impossible. If you have reason to not want attention from the government (for example, if you are not a citizen), then the best way to be as safe as possible is to not engage with any movement.

Myth # 2

"We have to identify the federal agent, police officer, or infiltrator, etc. in the group"

- It's not safe nor a good idea to generally speculate or accuse people of being infiltrators. This is a typical tactic that infiltrators use to shut movements down.
- Paranoia can cause destructive behavior.
- Making false/uncertain accusations is dangerous: this is called "bad-jacketing" or "snitch-jacketing."

Myth # 3

"Police officers have to identify themselves. Police officers can't lie to you."

- Undercover infiltrators could not do their job if they had to identify themselves.
- Police officers are legally allowed to lie to people – and do so routinely – to encourage compliance, both on the street and especially in interrogation. Police officers and other agents also present false evidence, including pictures, video, and audio to trick people into talking about other people.
- Government agents of all kinds can threaten you, your family, and your friends. The best defense is to not talk, not believe them, not cooperate, and ask others for help.

Myth # 4

"Security Culture guarantees my safety."

- Security Culture makes you safer, but any effective action can lead to repression.
- Nothing can guarantee safety, but Security Culture makes us more effective.
- Strict separation between the aboveground and any underground that exists or may come to exist helps protect people.

Security Culture Breaches

Behavior, not people, is the problem

- There are many behaviors that can disrupt groups or make them unsafe. Whether someone is a cop or not does not matter. Focus on addressing the behaviors.
- Some of the behaviors to watch out for are sexism, abusive behavior, gossip, and creating conflict between individuals or groups.

What to do if there are breaches of Security Culture

- Educate (tactfully and privately) and point people who breach Security Culture to further resources.
- Don't let violations pass or become habit.

- Chronic violators have the same detrimental effect as infiltrators. It is important and necessary to set boundaries. If a member consistently violates Security Culture, even after being corrected, they should be removed from the group for the safety of everyone.

Resources

- Deep Green Resistance security culture videos presented by Aric McBay
- Civil Liberties Defense Center website
- The Mysterious Rabbit Puppet Army presents: "Donny, Don't!", a security culture training skit (text transcript or 3.7 MB MP3)
- ***The following documents are a must-read for any activist.***
    - Agent At The Door: one-page guide to handling visits from government officials in the US. You may want to print this out and post it by your door.
    - You Have the Right to Remain Silent
    - Operation Backfire
    - Security Culture: A Handbook for Activists
- Computer security
    - Encryption Works: How to Protect Your Privacy in the Age of NSA Surveillance by the Freedom of the Press Foundation
    - PRISM BREAK – detailed list of software options.
- The Grand Jury Resistance Project provides useful information, including PDFs on A Few Facts About Grand Juries (1 page), Grand Juries Are An Abuse Of Power! (2 page brochure), and What You Should Know About Grand Juries (2 pages, plus example subpoena.)

Frequently Asked Questions

Q: Do you have lawyers willing to help us/advise us as we act?

A: We are currently building legal support for this purpose. We need volunteers for this and other tasks.

Q: What should I say if someone says: "I want to form an underground, join an underground, start a safehouse, etc."

A: Say: "We are an aboveground organization. We do not want to be involved. We do not answer anyone's questions about personal desire to be in or form an underground."

Immediately cut off conversation if there are breaches of security. Sometimes, you have to end the conversation.

Do not say, “the underground” – this could imply we are in contact with an already existent underground organization. Instead, use, “an underground (which may or may not exist).”