Security Culture

Contents

Security Culture is the most powerful tool to keep us in the fight. The pigs have their spies and they are ready to use them to defame, fracture, jail, and intimidate our movement — this is no bullshit. It doesn't matter if you're a church group bake sale volunteer or a militant environmental activist, if you've been spitting distance from an anti-war meeting, you've been spied on by your government. Keep all groups small and intimate, one is best although it might make you crazy; three is a the number to never exceed for actions; group together several threes for very big actions, but don't use these groupings for actual civil disobedience. Try to form affinity groups with those you have known for many years. This disperses the threat and the effect of infiltration.

But you still need to be careful, even in large groups. Take this advice seriously — you're not doing anybody any good if you're locked up without having done anything.

Main points:

- NEVER BRAG about past actions!
- NEVER USE NAMES when planning an action!
- Only discuss action with those who NEED TO KNOW!
- After an action, NEVER DISCUSS it with OUTSIDERS!
- NEVER ADMIT anything to the authorities, even for a deal when they claim others have ratted out! If you haven't ratted them out yet, they probably haven't ratted you out either.
- While you're at it, DON'T TELL THE AUTHORITIES ANYTHING!
- NEVER LIE about being in on an action or your part in an action!
- DON'T ASSUME that a friend of a friend is a friend!
- Keep involved members to a VERY SMALL group!
- ONLY work with a TRUSTED affinity GROUP!
- ONLY ALLOW those who would NEVER rat out the group INTO a TRUSTED affinity GROUP!
- ONLY DISCUSS action in OPEN AREAS with background noise!
- NEVER discuss action in HOMES, KNOWN MEETING AREAS, PUBLIC TRANSPORTATION or CARS!
- If busted use your right to REMAIN SILENT!
- If busted NEVER ARGUE or try to EXPLAIN yourself!
- NEVER! NEVER! **NEVER!** RAT out another activist!
- Be extra CAUTIOUS with ROMANTIC or SEXUAL PARTNERS!

- NEVER TRUST electronic ENCRYPTION or codes to keep your communication safe!
- ALWAYS CHECK your wallet and gear for incriminating documents and maps

---

Parts of what follows is updated material from the site Why-War.com.

Electronic Communication

A little story: I worked with a direct action group in ****** known as ***. **One member of *** who was new and did not know the protocols of security culture sent out an e-mail that indirectly implicated specific members of the group in an action that had happened in the area. His e-mail resulted in four arrests. Two people went to jail for six months.

E-mail is never safe. Ever. Listservs especially sire monitored daily by local police departments and the FBI. If you're planning a mass direct action event, you must use a spokescouncil meeting or other face-to-face organizing strategy. Never send specifics (date, time, or location) about a direct action over e-mail. Some e-mail is more secure. Hushmail provides encrypted e-mail service for its users that can be more secure than regular e-mail, and using an encryption program like PGP can greatly increase your security, but remember that Hushmail and any other email provider will give the private key and email contents to the cops with a just a phone call, no warrant needed, thanks to the (un)Patriot Act. Keep your private PGP encryption key block private and ready to securely delete and overwrite, not on any providers' servers! Even with what you think is good, hard crypto, it's never a good idea to talk about specifics over e-mail. Keep any discussion of direct action extremely vague, and never give the location and time. So you get up every day looking for your chance to make your voice heard. Where do you look? Why, Indymedia, infoshop and protest.net, of course! Well guess what? Someone else is reading those websites too.

Never trust any kind of encryption, nearly all codes have eventually been broken, they are only meant to slow down the opposing side!!

There is one kind of encryption that so far *if perfectly executed* is unbreakable. The trade off is that key exchanges and getting sufficiently random numbers are more involved. This type of encryption is known as a One-Time Pad http://en.wikipedia.org/wiki/One-time_pad. These can either be done with a ten sided dice shaken in a cup or a bingo number drum, a pencil and paper, or with a computer program http://www.scubaninja.eom/code/c/xor/ although computer generated pads are sometimes later found to not be truly random and can then be cracked, you or your computer program must also use a rotating mathematical algorithm that prevents letter frequency, word, and sentence pattern decoding attacks. The general idea with a OTP is that both the sender and the receiver have a set of "pads" filled with random data. Sending a message takes one "pad", which is then destroyed. This is the big tradeoff with OTPs: obviously, the unused pads must be kept secret, just like any other encryption key, but the used pads have to be disposed of properly, too. (Burned if paper, securely deleted if electronic.) Make sure you know what you're doing if you use this method. Secure deletion especially during a surprise raid is very difficult, hard disk platters are incredibly durable and take a long time to fully overwrite enough times, RAM memory chips which if quickly powered off and cooled may retain recoverable data for over an hour.

Websites

The State reads protest websites all the time. Why War's website has received hits from most branches of the military. Stealthiswiki.org has been mentioned in the record of the California state assembly, so you bet the piggies are reading it. If you post specific details about a direct action on the Internet, you can expect there to be cops there when you show up. I believe that the best way to organize is to call a spokescouncil meeting and post the information on Indymedia. Always remember that everything you say on the Internet is there forever. Don't make jokes. Even visually representing an attack on the president has cost one person a visit from the Secret Service.

Identity

Assume everyone is a cop. I am a cop. You are a cop. The only people you can assume are not cops are your mother (unless she is a cop) and your affinity group. If someone e-mails you saying they are from one group or another, they are a cop. (Not necessarily, in fact, probably not, but you need to treat them like they are.) Especially on the Internet, you can never assume anyone is who they claim they are. Nothing is less secure than the Internet, where anyone can read anything you say at any time. Still, after the passing of the Patriot Act, phones are not secure. Whistleblowers have exposed that communication companies have given the government direct links into our phone and data lines. They tapped our phones in Boston. The ACLU has its phones tapped. It's not that rare. Using cell phones to communicate at an action seems like a really good idea, and it can be. But cell phones are easily monitored, and the special operations cops have the ability to monitor cell phones in a certain area. So don't say, "Swarm the comer of 33rd and 5th!" Plan everything out ahead of time, and be able to say, "Are you coming?" or "Green team GO!" and have everyone know what that means. Body mods, drug use, and tattoos are by no means a sure sign of a person being on our side. Informants come in all shapes and sizes, and may be very convincing. Some are even trained by the military. (If you think that's a load of paranoid bull, just have a look here (http://www.democracynow.org/2009/7/28/broadcast_exclusive_declassified_docs_reveal_military) •)

Another measure of caution to use is to agree on a confidential codeword or codewords to identify others of your group. If a riot is ensuing and some guy is shouting "Asparagus!", other people might think he's a nut. Your group, however, will know he's one of yours.

Phones

For immediate actions, the phone can be fairly secure, if you can act before the police can react. However, unless you are using a payphone, this leaves your name implicated with whatever action you do. In general treat a payphone as if someone were listening. Never give specifics. There are ways to know if your phones are tapped, if you really want to know, but it's best always just to assume that they are. Many payphones are tapped in accordance with the PATRIOT Act. The police also have the ability to listen to you through your phone even if you are not on the phone at that moment. They have to the technology to do this unless your phone is unplugged. This is why pre-pay cellphones are popular with the ignorant activist. Unfortunately they are incredibly easy to track — much more dangerous than a pay phone.

Documents

Every activist must remember that even if they do remain silent their vehicle, gear, and person will be searched for documents and clues to identity them as well as indicate connection to past or present

illegal activity. Most people have a habit of making a filing cabinet of their wallet by keeping business cards of friends or businesses you frequent, at the least you cast suspicion on all of these people. Maps, trash, personal orgainser/phone number list books, matchbooks, business cards, campground or tourism directories, etc can all give away your plans, even more so the information in your mobile phone or SIM chip and laptop. Even unique equipment or clothing labels may give clues to the region of your origin, surely eliminate gear you have used on direct actions. A good plan is to leave behind your wallet and only take one piece of ID to events.

Fear

Perhaps the easiest (and most detrimental) time for security culture to break down is in the heat of a protest when the police begin their repression tactics. You see your friends being taken away by police and it is your first instinct to call out to them. Or perhaps the group you are marching with shatters and you feel the need to remind everyone of where your pre-planned re-convergence space is. It is at this point that your faith and trust in your friends is most severely tested; therefore, everyone should make the utmost effort to build these things beforehand.

Have a thorough briefing before an action (just like the Special Forces do!) Make sure everyone knows the plan *cold.* Work out any contingencies you can think of (remember Murphy's Law), so that if they occur, everybody's response is almost automatic. It's much easier to deal with a situation if you've gone over it beforehand with a cool head. Also be prepared for things to not go according to plan — they rarely do — and trust your friends to do what is needed. That's what it really comes down to.

There's a great mantra for fighting fear that's used in the book *Dune.* Maybe it will be of use to you as well:

I must not fear.
Fear is the mind-killer.
Fear is the little-death that brings total obliteration.
I will face my fear.
I will permit it to pass over me and through me.
And when it has gone past I will turn the inner eye to see its path.
Where the fear has gone there will be nothing.
Only I will remain.

As an aside: remember to walk, not run, at any group march, even in a serious retreat. Running can be the start of a stampede which can kill many activists.

Names

Don't use people's names at a direct action protest. If you want, use special nicknames come up with aliases or something, but concealing your identity from the authorities is important. You might not think they are listening, but they are. Another story: at a peace rally in ****town, the local radical groups held a spokescouncil meeting at the beginning of the rally to decide when we were going to break away from the main march. In the middle of our meeting, we were surrounded by police who then walked with us the entire way.

Appearance

Don't look sketchy. If you're having a spokescouncil meeting in a public place, take off your bandannas! Put away the red and black banners, steal a "Peace is Patriotic" sign from a nearby liberal,

whatever. Increasingly, the cops are targeting radical groups for arrest and "special treatment" (i.e. police brutality) and, increasingly, what the cops consider to be a radical group is becoming less and less radical. Black flags and radical banners are all well and good, but keep them out of sight while you're planning. Some of you might be saying, "Wait, take off our bandannas? That's such a bad plan!" In some ways, you're correct. As I said before, concealing your identity is important. The average American is photographed 300 times a day (every time you use an ATM, get gas, go into a convenience store, pay a toll, etc.). Protests are very well monitored by video and snapshots.

Masks

If you are engaging in autonomous civil disobedience (not a sit-in) and you don't plan on being arrested (i.e. you want to get away with it) you should conceal your face using a bandanna, or other cloth. When combined with a hat (Simple is best) and some sunglasses, this getup makes you nearly impossible to identify via facial recognition. Wearing a bandanna can make you a target for police, since they associate it with radicals, so only wear one if you are actually doing something illegal and concealing your identity makes sense. Gas masks and ski masks certainly conceal your identity well, but they look extremely militant, and tend to both incite police violence and frighten other protesters. Unless you plan on directly and forcibly confronting the police, I would not recommend wearing a gas mask. (If you think that there will be teargas, you can always have a pair of swim goggles and a bandanna soaked in apple cider vinegar in your pocket.) Also remember that the foam in ski masks and ski goggles will trap teargas and other gasses, after a while this will expose your face to more teargas than wearing nothing at all. Swimming goggles are therefore more advisable.

Safe Sex

One of the most difficult areas of security culture exists between partners in a sexual relationship.

There is an implied special bond and dissolution of barriers between those who spend their naked time together. If potentially important information is not shared, there is often a feeling of betrayal. It is best from the beginning of a sexual or romantic relationship to let your significant other know there are or may develop activities you are involved in that you are unable to share. If they are really cool with the cause and secure in themselves they should understand, if not you have to choose. Drop them or drop out of direct action.

The problem with many relationships between activists (and ordinary people too) is that the relationship ends after a time, this sometimes gets ugly if hearts are broken. It is not an unreasonable concern that a jilted lover might even turn to the pigs or talk too openly to get revenge. This includes exposing Internet pen names, turning over cell phone history, or capitalizing on any other one of the number of different privacy fallacies we have about our lives.

Another consideration is the sellout for ransom, a person may choose to make a deal and narc out the whole organization when their lover is threatened with serious punishment where they might stand strong for themselves, the pigs are famous for this blackmail deal, done in a secret way where the significant other may never even find out.

Short term relationships or even one night stands can be very dangerous, there are those cops and civilian narc types who have a kink for playing the spy while having a little naked fun in the sack with their target. Never discuss any involvement of any kind beyond generic politics at all with a short term relationship especially if it looks like trading insider info will get you sex.

There is wisdom in the idea of our cells having a professional expectation of no romance between activists, this is often an unrealistic expectation, each group must decide what is acceptable.

And don't forget to use a condom.

Tough Love

A danger that we don't often expect and that usually hurts the worst is the loving friend, parent, or close relative intervention bust. A naive and police state propaganda addicted person who full of "tough love" for the unsuspecting victim hopes to rescue them from dangerous radicalism may destroy their life forever by calling the police in hopes that this bust will set them on the straight path. The interventionist truly thinks that by turning the youngster in instead of them getting caught the victim will only get a slap on the wrist to scare them straight, much like taking a five year old shoplifter back to the store, but this leaves our young radical with a criminal record or worse fighting for their lives in prison, even juvies under 18. These 'helpful' intervention sell outs are often for drag use or shoplifting not even for radical action where we are often more secretive but once they pigs have permission to dig...

Unnecessary Criminal Activity

Do not become involved in activities like shoplifting, reckless driving, or narcotics if you are an activist. Do not permit members of your affinity group to engage in these activities, either. It is already easy enough for the police to blackmail us. Most busts for "domestic terrorism" are the result of shoplifting or traffic stops. Once someone has been released and heavy charges dropped it might be wise to insulate them from serious direct action as they may have made a deal and are now working for the other side in exchange for their continuing freedom. It is important to realize that alcohol and many drugs make you much more likely to open your mouth and blab about your activities, think truth serum here.

Practice

Remember to practice security culture with your friends. This is the hardest aspect of security culture for many of us to perfect. You've just finished a successful and awesome direct action! Yay! The first thing you want to do is tell all your friends about it. Chances are, your friends won't turn you into the cops. However, bragging/gossiping about direct action can be a chronic breach of security culture.

Tips

There are some things that you should NEVER talk about with people that you don't know very, *very* well on a personal basis:

- Your involvement or someone else's in a specific illegal direct action. The only exception is if you have already been convicted of that action, or if you are outside the jurisdiction of where that action took place, or if, beyond any doubt whatsoever, the statute of limitations has passed, so that you cannot be prosecuted for the action or used as a witness.
- Almost all the time, though, there are no exceptions. Don't tell anyone anything, ever. Even if you cannot be found guilty, talking about your past actions implicates you and increases police observation directed in your and your colleagues' direction. Even if you're being investigated, every lead you release could be the one that ends up getting you screwed over.
- Your involvement or someone else's in an underground group (i.e. a group that has claimed actions for the Earth Liberation Front, etc.)
- Someone else's knowledge of an illegal direct action.

- Specific plans for future direct actions. With a good security culture, everyone is on a need-to-know, don't-ask-don't-tell basis. The less you know about an action that you will not be involved in, the safer you and the people engaging in that action will be. Obviously you can discuss future actions with your affinity group, but do so in a safe place and manner.

Planning

When discussing plans for a radical direct action with your affinity group, do not discuss them in a place likely to be monitored (i.e the place you usually meet, an activist's car, Unitarian churches, radical bookstores, etc.). Find someplace safe for your discussion. There are some things that we as humans tend to do that can be extremely risky for us as activists. Using activism as a social device can be detrimental to security culture. There are liars: people who claim to have engaged in illegal actions in order to impress others. This is not okay. Those people are putting themselves and the people they lie to in danger by breaking security culture in this way. Bragging to your friends, I can't emphasize enough, is dangerous. One on one, in a safe location, it is okay to talk about less radical direct actions, but only talk about secure things with people who know about security culture and won't go and gossip it to others. This brings us to gossiping. If you've heard anything about a direct action that you're not involved in, don't say anything about it to anyone. You will jeopardize your security and the security of those planning the action.

Security of Your Security Culture

Security culture is not a spy game or a joke. Pretending to have an overdeveloped sense of security culture in order to impress others is no different than bragging about an action. This is not "I could tell you but I'd have to kill you." If someone asks you a question that you don't want to answer, or if you think someone is talking about something that they shouldn't be talking about, just change the subject.

Conclusion

Before I end we should also note that there are informants out there. They infiltrate activist groups, (and sometimes even activist affinity groups) and jeopardize (intentionally) everyone's security. It can be hard to distinguish between new members of a group who want to learn about what's going on and don't know much about security culture and infiltrators who are trying to gather enough information to have you all arrested. If you think your group may have been infiltrated, check out the Security Survival Skills guide produced by the Collective Opposed to Police Brutality. It's the most extensive guide to security culture that I've found on the web and it has a section that explains how to identify counterinsurgents within the ranks.

This is by no means a complete and definitive guide to security culture. Again I urge you to read the Security Survival Skills (http://www.why-war.com/files/2003/09/activist_security.html) guide produced by the Collective Opposed to Police Brutality.

Always remember this: Just because we're non-violent doesn't mean that the police don't see us as a threat, or that they won't pretend to see a threat if it suits them. It also doesn't mean that we will not be charged with violent crimes if arrested. You can be charged for assault if you even brush against a police officer, for carrying a weapon if you have a pencil, and for reckless endangerment if you hang a banner on a building.

Maintaining a tight security culture is essential for creating a cohesive, safe, and effective movement based on the principals of trust and solidarity. This guide may seem harsh and paranoid, and you should

always use reason. You're probably not gonna get yourself in trouble by talking about some snake-march you participated in, but always be thinking, "Would I say this to a cop?"

Security Culture

Last updated: 26 June 2011

stealthiswiki.com