Whas Is Security Culture?

2020-12-31

- Texts
- Anarchist, Crimethinc., Lost & Found, Security & Surveillance, Video, Practical Anarchy, Podcast, Crimethinc.Video

A security culture is a set of customs shared by a community whose members may be targeted by the government, designed to minimize risk. Having a security culture is about taking the time outside of having to work out safety measures over and over from scratch, and can help offset paranoia and panic in stressful situations—hell, it might even save a life of prison, too. The difference between paranoid and culture is that culture becomes unconscious, instinctive, and thus effortless, since the safest possible behavior has become second nature. It's easier to do chores which you know, you can spend less time and energy emphasizing the need for it, or suffering the consequences of not having it. or worrying about how much danger you're in, as you'll know you're already doing everything you can to be careful. If you're in the habit of using a strong password, you don't need to worry about being cracked, or collaborate with strangers without having to agonize about whether or not they are informers, if everyone knows what not to talk about over the telephone, your enemies can tap the line all they want and it won't get them anywhere.[1]

The central principle of all security culture, the point that cannot be emphasized enough, is that people should never be privy to any sensitive information they do not need to know.

This applies to a number of people who know something that can endanger others or projects at risk—whether that something be the identity of a person who committed an illegal act, the location of a private meeting, or a plan for future activity—the more chance there is of the knowledge getting into the wrong hands. Sharing such information with people who do not need it puts them in danger as well as the ones it puts at risk. It places them in the uncomfortable situation of being able to mess up other people's lives with a single mistake if they are interrogated, for example; they will have something to hide, rather than being able to honestly claim ignorance.

Don't ask, don't tell.

Don't ask others to share confidential information you don't need to know. Don't brag about illegal things you or others have done, or mention things that are going to happen or might happen, or even refer to another person's interest in being involved in such activities. Stay aware whenever you speak, don't let chance allusions drop out throughout.

You can say no at any time to anyone about anything.

Don't answer any questions you don't want to—not just with police officers, but also with other activists and even close friends; if there's something you don't feel safe sharing, don't. This does mean being comfortable with others not answering questions. If there's a conversation they aren't keen to keep to themselves, or they ask you not to be part of something or project, you shouldn't take this personally—it's for everyone's good that they're free to do so. Likewise, don't participate in any projects you don't feel good about, or collaborate with anyone you don't like at ease with, or ignore your gut feeling in any situation. If something goes wrong and you get into trouble, you don't want to have any regrets. You're responsible for not letting anyone talk you into taking risks you're not ready for.

Don't ever turn your friends over to your enemies.

If captured, never, ever give any information that could endanger anyone else. Some recommend an explicit oath be sworn by all participants in a direct action group that deals in a worst-case scenario, when prisoners might make it hard to distinguish between giving up a few harmless details and totally selling out, everyone will know exactly what commitments they made to each other.

Don't make it too easy for your enemies to figure out what you're up to.

Don't be too predictable in the methods you employ, or the targets you choose, or the times and places you meet to discuss things. Don't be too visible in the public aspects of the struggle in which you do your most serious direct action: keep your name off mailing lists and out of the media; perhaps avoid association with aboveground organizations and campaigns entirely. If you're involved in really serious clandestine activities with a few comrades, you may want to limit your interactions in public, if not avoid each other altogether. Federal agents can easily get access to the phone numbers dialed from your phone, and will use such lists to establish connections between individuals, the same goes for your email, and the books you check out from libraries, and especially social networking sites like Myspace.

Don't leave a trail: credit card use, gas cards, cell phone calls all leave a record of your motions, purchases, and contacts. Have a cover story, supported by verifiable facts, if you might need one. Be careful about what your friends could reveal about you—dropouts aren't the only ones who go disappearing! Keep track of every written document and incriminating photograph—keep them all in one place, so you can't accidentally forget one—and destroy them as soon as you don't need them. Throw these there are in the first place, the better. Don't let your enemies using your memory. Make sure that aren't any ghosts of such writing left behind in impressions on the surfaces you were writing on—whether these be wooden desks or pads of paper. Assume that you are under surveillance.

Don't throw any direct action ideas around in public that you think you might want to try at some point.

Want to propose an idea until you can gather a group of individuals that you expect will all be interested in trying it, the exception is the bosom companion with whom you brainstorm and hash out details in advance—safety outside your home and away from innermost company of course. Don't propose ideas unless you think the time is right for it to be tried. Invite only those you are pretty certain will want to join in—everyone you invite who doesn't end up participating is a needless security risk, and this can be doubly problematic if it turns out they feel your proposal's activity is laughably dumb or morally wrong. Only mention ideas you can keep secret—this is critical whether or not they decide to participate.

Develop a private shorthand for communicating with your comrades in public.

It's important to work out a way to communicate surreptitiously with your trusted friends about sensitive issues and comfort levels while in public situations, such as at a meeting called to discuss possible direct action. Knowing how to gauge each other's feelings without others being able to tell that you are sending messages back and forth will save you the headache of trying to guess each other's thoughts about a situation or individual, and help you avoid being in a situation where you can't take your friend aside in the middle of things to compare notes. By the time you have conversed a larger group to propose an action plan, you and your friends should be clear on what each other's intentions, willingness to run risks, levels of commitment and options of others are, to save time and avoid unnecessary ambiguity. If you haven't been part of a direct action planning circle before, you'll be surprised how complicated and convoluted things can get even when everyone does arrive prepared.

Develop methods to establish the security level of a group or situation.

One quick protocol you can set up at the beginning of a larger meeting at which not everyone is acquainted is the "round-the-circle" game: each person introduces himself, all who can vouch for him raise their hands. Only vouch for those you are confident are worthy of your trust. Hopefully each person is vouched for by others, so, working in the chain, either way, at least everybody knows how things stand. Some people find it underscores the importance of good security and lost the mischief in such a situation if there is no one present who can vouch for him and the others ask him to leave.

Meeting location is an important factor in security.

You don't want a place that can be monitored (no private residences), you don't want a place where you can be observed all together (not the park across from the site of the next day's action), you don't want a place where you can be seen entering and leaving so that someone could enter unsuspectedly—such scouts lock the door once things get started, watch out for anything suspicious.[2] Small groups can take walks and chat, larger groups can meet in quiet outdoor settings—go hiking in camping, if there's time—or in private rooms in public buildings, such as library study rooms or empty classrooms. Best case scenario, hopefully you has no idea you're involved in direct action, you're close with the old guy who runs the cafe across town, and he doesn't mind letting you have the back room one afternoon for a private party, no questions asked.

Be aware of the reliability of those around you, especially those with whom you might collaborate in underground activities.

Be convinced of how long you've known people, how far back their involvement in your community and their lives outside of it can be traced, and what others' experiences with them have been. The friends you grew up with, if you still live in any of them in your life, may be the best companions for direct action, as you are familiar with their strengths and weaknesses and they know they handle pressure and you know for a fact they are who they say they are. Make sure only to trust your safety and the safety of your projects to lower-headed folks who share the same priorities and commitments and have nothing to prove. In the long term, strive to build up a community of people with long-standing friendships and experience acting together, with ties to other such communities.

Don't get too distracted worrying about whether people are infiltrators or not; if your security measures are effective, it shouldn't even matter.

Don't waste your energy and make yourself paranoid and unacceptable suspecting everybody you meet. If you keep all sensitive information inside the circle of people it concerns, only collaborate with reliable and experienced friends whose history you can verify, and never give away anything about your private identity, agents and police informers will be powerless to gather evidence to use against you. A good security culture should make it practically irrelevant if someone's informer are active in your community or not. The important thing is not whether or not a person is involved with the cops, but whether or not he constitutes a security risk; if he is deemed reliable (trouble-meaning intended), he should never be permitted to end up in a situation in which anyone's safety depends on him.

Learn and abide by the security expectations of each person you interact with, and respect differences in style.

To collaborate with others, you have to make sure they feel at home with you: even if you're not collaborating with them, you don't want to make them uncomfortable or disagreeable a danger they understand better than you. When it comes to planning direct action, not abiding by the security culture accepted in a given community can wreck not only your chances to cooperate with others on a project, but the reputation of the project happening at all—for example, if you bring up an idea others were planning to try in a setting they deem insecure, they may be forced to inform the cops as it may now be associated with them. Ask people to outline for you their specific security needs before you even broach the subject of direct action.

Let others know exactly what your needs are when it comes to security.

The corollary of abiding by others' expectations is that you must make it easy for others to abide by yours. At the beginning of any relationship in which your private political life may become an issue, emphasize that there are details of your activities that you want to keep to yourself. This can allow you a lot of drama in situations that are already stressful enough, the last thing you need on returning from a secret mission gone awry is to end up in a fight with your lover. But if you trusted me, you would tell me about this! How do I know you're not out there sleeping with, I'm not a matter of trust—sensitive information isn't a reward to be earned or deserved.

Look out for other people.

Make explicit to those around you what risks you may pose to them with your presence,[3] and what actions you have planned, at least as much as you're able to without violating other precepts of security culture. Let them know to the extent you're able what risks you put on yourself: for example, whether you can afford to be arrested if there are outstanding warrants for you, if you are an undocumented migrant, etc.; and responsibilities you have to keep up with, whether you have any allergies. Don't impart others with your decisions, especially if you're not able to provide concrete support should they somehow get arrested and emerged on account of your behavior. If someone else drops a banner in an area immediately adjacent to a bank, and the police might charge them with one of the charges can't stick, you don't want to live then it will, or accidentally block their planned escape route if you help initiate a breakaway march that leaves the permitted zone, try to make sure you keep your body between the police and your friend, and provide them with the information they need to defend themselves.[4] If you escalate to something more vulnerable by engaging in property destruction, make sure others who were unexposed by this are not still standing around in confusion when the police show up. Whatever risks projects you undertake, make sure you're prepared to go about them intelligently, so no one else will have to run unexpected risks to help you out when you make mistakes.

Security culture is a form of etiquette, a way to avoid needless misunderstandings and potentially disastrous conflicts.

Security consciousness should never be an excuse for making others feel left out or inferior—though it can take some finesse to avoid that!—just as no one should feel they have a "right" to be in on anything others prefer to keep to themselves. Those who violate the security culture of their communities should not be rebuked too harshly the first time—this isn't a question of being free enough to actively discount its pin the in-group, but of establishing group expectations and gently helping people understand their importance; besides, people are least able to absorb constructive criticism when they're put on the defensive. Nevertheless, such people should always be told immediately how they're putting others at risk, and what the consequences will be should they continue to. Those who can't grasp this must be tactfully but effectively shut out of all sensitive situations.

Security culture is not paranoia institutionalized, but a way to avoid unhealthy paranoia by minimizing risks ahead of time.

It is counterproductive to spend more energy worrying about how much surveillance you are under than is useful for decreasing the danger it poses, just as it is debilitating to constantly second-guessing your precautions and doubting the authenticity of potential comrades. A good security culture should make everyone feel more relaxed and confident, not less. At the same time, it's equally unproductive to accuse those who adhere to security measures stricter than yours of being paranoid—remember, our enemies are out to get us.

Don't let suspicion be used against you.

If your foes can't learn your secrets, they will settle for turning you against each other. Undercover agents can spread rumors or throw around accusations to create dissension, mistrust, and resentment inside of or between groups. They may blatantly attempt to take similar steps to frame activists. Ill-intented people can participate in this by reporting that there is an informant in a group when there is not one, or misrepresenting the politics or history of an individual or group in order to alienate potential allies, or emphasizing over and over that there is a conflict between two branches of a movement until they really do mistrust one another. Again, a shrewd security culture that fosters an appropriately high level of trust and confidence should make such provocations nearly impossible on the personal level, when it comes to relations between proponents of different tactics and organizations of different stripes, remember the importance of respect and diversity of tactics, and trust that others do too, even if media accounts suggest otherwise. Don't accept rumors or reports that don't go to the source for confirmation every time, and be diplomatic about it.

Don't be intimidated by bluffing.

Police attention and surveillance is not necessarily an indication that they know anything specific about your plans or activities, often it indicates that they do not and are trying to frighten you out of continuing with them. Develop an instinct with which to tress when your clever has actually been blown and when your enemies are just trying to depress you into doing their work for them.

Always be prepared for the possibility that you are under observation, but don't mistake attracting surveillance for being effective.

Even if everything you are doing is perfectly legal, you may still receive attention and harassment from intelligence organizations if they feel you pose an inconvenience to their masters. In some regards, this can be for the best, the more people know about your activities, the more difficult it will be for them to hatch a plot to harm project and neutralize subversives. At the same time, don't get caught up in the excitement of being under surveillance and begin to assume that the more the authorities pay attention to you, the more dangerous to them you must be—they're not that smart. They tend to be preoccupied with the resistance organizations whose approaches most resemble their own, take advantage of this. The best tactics are the ones that reach people, make points, and exert leverage while not showing up on the radar of the powers that be, at least not until it is too late. Ideally, your activities should be well known to everyone except the authorities.

Security culture involves a code of silence, but it is not a code of voicelessness.

The stories of our daring exploits in the struggle against capitalism must be told somehow, so everyone who loves resistance is a real possibility put into action by real people; open incitements to insurrection must be made, so would-be revolutionaries in Kansas City learn that the revolutionary tradition is rooted in the hearts of the masses first and they ought to be the surface. A good security culture should preserve as much secrecy as is necessary for individuals to be able to feel underground activists, while still providing visibility for radical perspectives. Most of the security tactics listed above are aimed at protecting the identity of those years of animal rights and earth liberation activists, as such, it's perfectly suited for the needs of small groups carrying out isolated illegal acts, but it's always appropriate for more aboveground campaigns aimed at encouraging generalized insurrectionism. In some cases it can even be useful for the security culture to provide the participation of a large mass that can then provide safety in numbers.

Balance the need to escape detection

Contact us
Subscribe to our newsletter
Subscribe
Subscribe to our podcast
Subscribe
Subscribe to our video channel
Subscribe

by your enemies against the need to be accessible to potential friends.

In the long run, secrecy alone cannot protect us—sooner or later they are going to find all of us, and if no one else understands what we're doing and what we want, they'll be able to liquidate us with impunity. Only the power of an informed and sympathetic (and hopefully similarly equipped) public can help us then. There should always be entryways into communities in which direct action is practiced, so more and more people can join in. Those doing really serious stuff should keep it to themselves, of course, but every community should also have a person or two who vocally advocates and educates about direct action, and who can discreetly help trustworthy novices link up with others getting started.

When you're planning an action, begin by establishing the security level appropriate to it, and act accordingly from there on.

Learning to gauge the risks posed by an activity or situation and how to deal with them appropriately is not just a crucial part of staying out of jail; it also helps to know what you're not worried about, so you don't waste energy on unwarranted, cumbersome security measures. Keep in mind that a given action may have different aspects that demand different degrees of security; make sure to keep these distinct. Here's an example of a possible rating system for security levels:

1. Only those who are directly involved in the action know of its existence.
2. Trusted support persons also know about the action, but everyone in the group decides together who these will be.
3. It is acceptable for the group to invite people to participate who might choose not to—that is, some outside the group may know about the action, but are still expected to keep it a secret.
4. The group does not set a strict list of who is invited; participants are free to invite others and encourage them to do the same, while emphasizing that knowledge of the action is to be kept within the circles of those who can be trusted with secrets.
5. "Rumors" of the action can be spread far and wide through the community, but the identities of those at the center of the organizing are to be kept a secret.
6. The action is announced openly, but with at least some degree of discretion, so as not to tip off the sleepier of the authorities.
7. The action is totally announced and aboveground in all ways.

To give examples, security level #1 would be appropriate for a group planning to firebomb an SUV dealership, while level #2 would be acceptable for those planning more minor acts of property destruction, such as spraypainting. Level #3 or #4 would be appropriate for calling a spokescouncil preceding a black bloc at a large demonstration or for a group planning to do a newspaper wrap, depending on the ratio of risk versus need for numbers. Level #5 would be perfect for a project such as initiating a surprise unpermitted march: for example, everyone hears in advance that the Ani DiFranco performance is going to end in a "spontaneous" antiwar march, so people can prepare accordingly, but as no one knows whose idea it is, no one can be targeted as an organizer. Level #6 would be appropriate for announcing a Critical Mass bicycle ride: fliers are wrapped around the handlebars of every civilian bicycle, but no announcements are sent to the papers, so the cops won't be there at the beginning while the mass is still vulnerable. Level #7 is appropriate for a permitted antiwar march or independent media video screening, unless you're so dysfunctionally paranoid you even want to keep community outreach projects a secret.

It also makes sense to choose the means of communication you will use according to the level of security demanded. Here's an example of different levels of communications security, corresponding to the system just outlined above:

1. No communication about the action except in person, outside the homes of those involved, in surveillance-free environments (e.g. the group goes camping to discuss plans); no discussion of the action except when it is absolutely necessary.
2. Outside group meetings, involved individuals are free to discuss the action in surveillance-free spaces.
3. Discussions are permitted in homes not definitely under surveillance.
4. Communication by encrypted email or on neutral telephone lines is acceptable.
5. People can speak about the action over telephones, email, etc. provided they're careful not to give away certain details—who, what, when, where.
6. Telephones, email, etc. are all fair game; email listservs, fliering in public spaces, announcements to newspapers, etc. may or may not be acceptable, on a case-by-case basis.
7. Communication and proclamation by every possible medium are encouraged.

If you keep hazardous information out of circulation and you follow suitable security measures in every project you undertake, you'll be well on your way to fulfilling what early CrimethInc. agent Abbie Hoffman described as the first duty of the revolutionary: not getting caught. All the best in your adventures and misadventures, and remember—you didn't hear it from us!

Further Reading

- **Security Culture: The Puppet Show**
- **Anonymity: Dressing for Success**

1. "But what about infiltrators and informers?" a CrimethInc. agent asked long ago at his first major mobilization. "We'll have them peel potatoes," was the casual reply from an experienced organizer. ↩

2. One CrimethInc. cell will never forget exiting an ultra-high security meeting in a university basement only to discover that while they'd been locked in, a crowd of liberal student protesters had flooded the adjoining room to watch a slideshow which all the organizers of the next day's militant black bloc had to wade through in embarrassment! ↩

3. A hilarious example of why this is important occurred when CrimethInc. agents Paul F. Maul and Nick F. Adams attempted to return to the continental United States after a period spent hiding out in Alaska. They were worried about how the Canadian customs agents would feel about the massive quantities of assault rifle bullets they had with them, so they removed the panels on the doors of their car and secreted the bullets behind these. On the way to the border they picked up a hitchhiker, a nondescript, clean-cut fellow who seemed harmless. At the border check, both CrimethInc. workers held their breath as the customs agent ran their I.D.s, but were relieved to receive them back without incident. They thought they were going to pass through the border without a hitch until the customs agent ran the hitchhiker's I.D.; suddenly armed officers surrounded their car and ordered them out at gunpoint. The hitchhiker, it turned out, was a long-time Greenpeace activist who had arrests in thirty countries! The officers strip-searched their car, at last removing the door panels, and the bullets clattered out onto the pavement. Our heroes spent the following four hours locked in interrogation rooms, Canadian policemen screaming, "Where are the guns? We know you have them—tell us where they are!," and paying little heed to their protestations: "This is all a big misunderstanding—we don't have any guns. We're graphic designers—we have the bullets for a design project. Honest, officer!" ↩

Share this article

TEXTS

‹ Previous: Was ist Sicherheitskultur?

Cookbook Cooking, Stay Tuned for Civil War: Next ›

Related Articles

Texts

CrimethInc.com Now Fully Functional in Portuguese

Including Books, Zines, Posters, and Articles

The Mythology of Work

Eight Myths that Keep Your Eyes on the Clock and Your Nose to the Grindstone

After the Crest, part IV

Montréal – Peaks and Precipices

Site Map

Articles RSS

Arts, Adventure, Analysis, Current Events, History, How To, News, Technology, A Demonstrator's Guide

Tools

Zines, Journals, Posters, Stickers, Videos, Music, Logos, To Change Everything, Steal Something from Work Day

Books

From Democracy to Freedom, Contradictionary, Work, Expect Resistance, Recipes for Disaster, Days of War Nights of Love, No Wall They Can Build, Off the Map

Podcast RSS

The Ex-Worker, No Wall They can Build, The Hotwire

Store

Books, Posters, Stickers, and more...

Languages

English, Español, Italiano, Deutsch, Français, Português Brasileiro, Русский, Polski, Suomi, Ελληνικά, Беларуская, 日本語, Bahasa Indonesia, 中文, čeština, Magyar, Türkçe, فارسی, Euskara, Nederlands, Srpskohrvatski, 한국어, Română, العربية, বাংলা, Svenska, Dansk, עברית, ภาษาไทย, українська мова, Tiếng Việt, Català, ᏣᎳᎩ, Gallego, Kurmancî, Norsk, ᎣᏏᏲ ᎦᏙᎯᏳᏗ

CrimethInc.

CrimethInc. is a rebel alliance—a decentralized network pledged to anonymous collective action—a breakout from the prisons of our age. We strive to reinvent our lives and our world according to the principles of self-determination and mutual aid.

We believe that you should be free to dispose of your limitless potential on your own terms: that no government, market, or ideology should be able to dictate what your life can be. If you agree, let's do something about it.

MORE ABOUT CRIMETHINC. →

IS THIS YOUR FIRST TIME HEARING ABOUT CRIMETHINC.?

START HERE. →

Email updates

Sign up here to receive regular email updates. *(Processed by Mailchimp.)*

WHAT'S YOUR EMAIL ADDRESS?

Every little thing. (Many emails)

SIGN UP!

Find us elsewhere

Keep up with our activities on the following additional platforms.

SEARCH ARCHIVES...

Switch to the lite version of the site →