Security: Culture, Relations, & Technology

An Activist 101

A Duck wrote most of this, with some help from their flock. You should review multiple resources and verify everything inside on your own. Anyone who claims to have all the answers should be doubted. Even ducks.

I hope I'm not the bearer of bad news, but I'm going to say it outright:

Fascism is upon us.

No longer can we deny that it has been creeping in; the current state of the United States is one of authoritarian oligarchical rule.

With this in mind, it's time to think about what that means as organizers and activists for our digital and organizational security.

Let's look at some of the things we know:

- We know that the tech oligarchs have bent the knee and kissed the ring of the Trump Administration.
- We know that anything that we don't control directly is susceptible to tampering.
- We know that the state has always looked to meddle in the affairs of activists and organizers.
- We know that in the first go-round, the Trump Administration has used the full weight of the government against activists and those he found inconvenient.

So what do we do? *We keep each other safe.* It's always been the case that we have to rely on each other, because that's all there is.

How do we keep each other safe? That's a question with many answers! So, let's get into it.

What Is Security Culture?

There are quite a few definitions of security culture, if you do a quick web search. The definitions will vary based on the circles you run in—the military, law enforcement, activists, and corporations all have conceptualizations of what security culture is; and they are all, to varying degrees, at least partially correct.

The definition I'd like you to think about as we move through this guide is this:

> A security culture is a set of customs shared by a community whose members may be targeted by the government or other threats, designed to minimize risk[1].

Three aspects to consider:

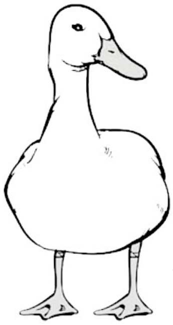
1) Security culture refers to the **customs** we follow. It's not a checklist you can adhere to (although checklists help!), it's not a one-and-done thing. It's a living practice that responds to the threats and situations we find ourselves in, and it relies on normalizing taking care within your cadre, affinity group, or network.

[1] https://crimethinc.com/2004/11/01/what-is-security-culture

2) It involves **community**. A single individual may have the strictest sense of security, but a single individual does not create a community, or a culture. Any project or group is as secure as its least secure member.

3) Security culture is about the **minimization** of risk. We can't eliminate it completely; we can only work together to make ourselves less of an easy target, and keep each other safe; and, have ideas of what do to if and when those risks manifest.

Threat Modeling



Before you get into taking any sort of steps to make yourself "secure", start thinking about what it is you're trying to secure yourself[2] against, and the chances of that thing happening. That is the basic idea of *threat modeling*, which can be defined as:

> A process by which potential threats can be identified and enumerated, so that countermeasures can be developed and implemented.

That sounds kinda complicated and technical. But it's actually something we generally do every day, just in normal life.

For most humans just existing in the world, we want to keep our bodies safe, and the most common threats are going to depend on where we

[2] yourself being your actual self, but also your group's activity, your information, whatever it is you need to keep safe.

are. If I'm in my home, I might prioritize shoveling snow and de-icing the sidewalk; I could fall and hurt myself. The threat is falling; the countermeasure is shoveling and de-icing.

Being reasonable about the threats that exist helps to allow me to do what I need to do—if I'm in the middle of New York City, my threat model just doesn't include a grizzly bear, for instance.

Being an activist or organizer gives you a different set of threats to consider—threats that you may not have been aware of, thought were just a myth, or didn't believe could be a threat.

There are a lot of resources to consult when considering what threats you might encounter. Talking to other activists and organizations, looking at history, reading the news, and talking with your comrades can all help to identify what threats might exist for your project.

Thinking about activist projects generally, here are some things I think about when considering my threat model:

1) **What methods am I using to accomplish my task?**
   (Is it above-board? Does it need to be underground? This will change your threat model.)

2) **Who needs to know about the project?**
   (If you're raising money for a bail fund, you want EVERYONE to know about the project. If you're [REDACTED], you don't want ANYONE to know about the project, save those directly involved.)

3) **Who needs to be involved in the project?**
(Limiting who you give access to is sometimes critical, sometimes not. There's a difference between, say, Food Not Bombs versus helping people get abortions.)

4) **Who'd like to see the project fail?**
(In a lot of respects, "The State" is always the answer, if it's a leftist endeavor; but also, different projects are going to attract different detractors. Are you more worried about police showing up to your protest, or counter-protesters?)

5) **What technologies am I using to accomplish my project?**
(By technologies, I don't just mean digital tech, I mean technologies broadly: tools, communication methods, etc.)

6) **What strengths and weaknesses do those technologies afford?**
(What other tools are possible that do similar things? What trade-offs are there if I use other technologies?)

7) **What have I done in the past or said in the past in a public sphere that endangers this project?**
(Public means literally anything on the internet, even private chats. Assume every space is monitored by feds, whether as participants or by subpoena later.)

8) **What methods of attack do detractors have to disrupt the project?**
(Dialogue often about this, and update what this means in your head frequently over the course of a project.)

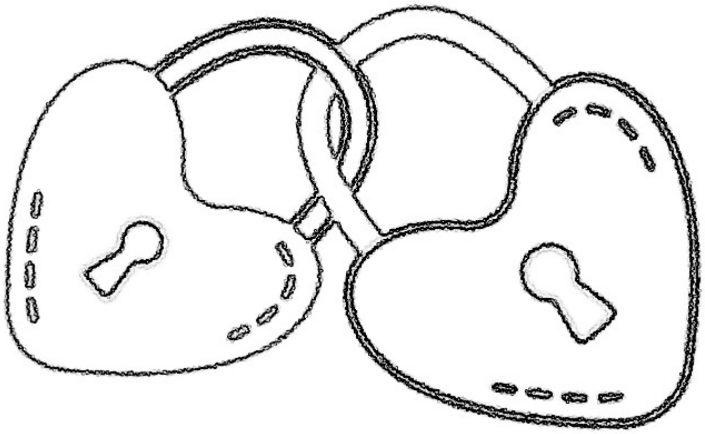
9) **What steps can I take to secure these project based on the things I've identified above?**
(We'll get to some answers to this question here in this guide!)

Relational Security

If this isn't something you're super familiar with, that's okay. Or, if you're familiar with it as a concept coming from the mental healthcare—well, that's not quite the same concept that I'm referring to. Let me explain.

Years ago, a group of activists—a majority of whom were women, non-binary, or queer—decided that what passed for security culture needed a reexamination through a feminist lens. After a lot of reading, discussing, and evaluating, a definition emerged:

> Relational Security is the honoring of human relationships, the things we do all the time, as both complex and the basis for creating liberatory and sustainable organizations, communities and movements.



From this definition, we can see that relational security involves itself with human relationships—how people interact, and how that interaction can increase or decrease security. It acknowledges the complexity of power, privilege, oppression, and hierarchy in our lives, and helps to bring some of these things to light as we move through the world. Relational security, at its foundation, asks you to evaluate disruptive and oppressive behavior as security threats and look for ways forward that prioritize caring for relationships so we can build stronger organizations and movements.

As you're organizing, start thinking about:

1) **What's the goal of the group?**
(If you don't have a super defined goal yet, that's okay.)

2) **What criteria qualifies a person to be in this group?** ('Whoever wants to show up' is a valid criteria for a union picket, but if your group exists to hack a government, the qualifications are going to be extra stringent!)

3) **How does that criteria relate to the goal of the group?**
(There should definitely be a relationship between the two.)

4) **What criteria means a person is automatically barred from this group?**
(There are always valid reasons people would be barred, but it's important to be explicit with it. Don't take things for granted.)

5) **How does that criteria relate to the goal of the group?**

(Being able to articulate how membership criteria is affected by group goal is a useful to avoid bias and set group norms around culture and behavior.)

6) **What biases exist that prevent people who fall within those parameters from being accepted?**
(This is where you, as the organizers, are examining your bias to ensure that you're not leaving people out who might have useful skills and perspectives to bring to organizing.)

This is not a comprehensive list, but hopefully it starts you thinking about who you let in, and why. Charisma, vibes, and resources all contribute to disruptors gaining the ability to access groups and cause chaos. Having criteria—that you revisit with the group regularly—can help to ensure that those that join you are there for the right reasons. And remembering that the point of activism (from a leftist context) is to care for each other, challenge the status quo, and create positive social change. Being aware of behaviors that do the opposite—show a lack of care, maintain the status quo, create negative change—can help to identify disruptors in our midst.

Speaking of disruptors:

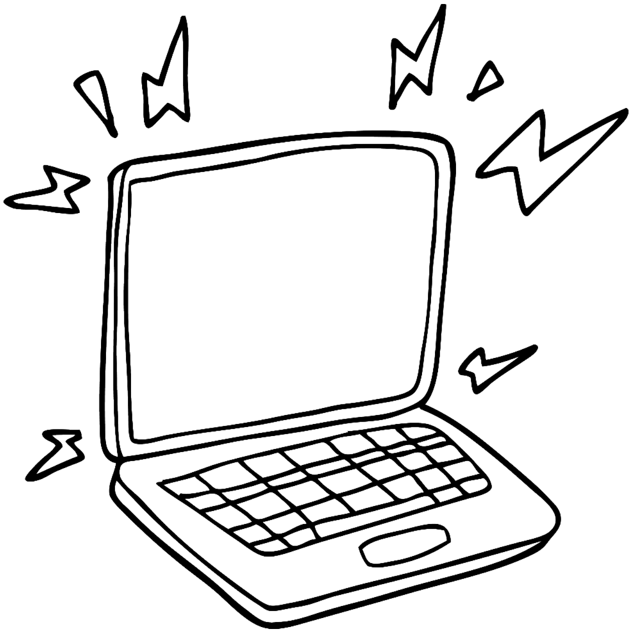
Disruption is disruption. Whether the instigator is an undercover cop, a right-wing nut-job, or just someone who enjoys sowing chaos, it's toxic to groups. It doesn't matter if they're a state agent, if they're doing the state's work.

This disruption can often come in the guise of misogyny, racism, ablism, and other -isms that seek to divide and oppress.

To combat this disruption, create cultural norms around addressing conflict outright, being anti-oppressive, and learning together.

At the same time, badjacketing (also known as snitchjacketing) is a practice of accusing someone of being an informant—usually with little-to-no evidence—to disrupt the group. False accusations can be as harmful to a group as intended disruption and real informants.

Cybersecurity



Cybersecurity is one of the most abused and misunderstood aspects of security for activists. Because of the difference in threats, things you do to be secure in your technology will look different than it would for a workplace or online shopping or dating or however else you might use technology.

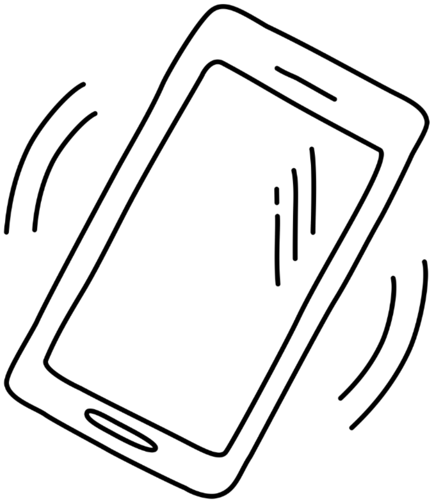
There are many tools available to help.

- VPNs[3] and Tor will hide where you're accessing internet resources from.
- Encrypted chat, email, and document storage will make communications more secure.
- Non-corporate email and document storage, or email based outside of the United States, will make it more difficult for government actors to access your data.

[3] Not every VPN is going to be appropriate. Make sure that it doesn't keep logs, and use one based outside the United States. Mullvad VPN is one of a few highly regarded VPNs for activists at the time of writing.

- ► Turning off tracking, and using browser extensions to minimize what information about you is being shared from site to site, will mean there's less data about your for entities to collect. Look for guides on being ad-free for ideas.

But cybersecurity tools are only as good as their adoption. There are many, many tools available that could make us *extremely* secure; but, the trade-off is that they're complicated to set up, requiring technical knowledge that not everyone has access to; inconvenient to use; and, aren't as widely known by the people we need to communicate with. The more complicated they are, the more of a chance you have of creating hidden vulnerabilities.



Phones are a whole *thing*. There are apps that are more secure or less secure that folks talk about; there are operating systems (iOS, Android and its variations) that have detriments and benefits. But really, one of the best tools we can use to keep ourselves cybersecure is: ***leave the phones at home when meeting.*** GPS coordinates and other metadata can not only identify where you've been, but can also paint a picture of who you meet with. This information has been used to incriminate otherwise innocent people. *Social Network Analysis*[4] (or social mapping) is a tool the government uses to identify networks of activists—and has, since the days of the Black Panthers and before. But now, with phones and apps constantly keeping tabs on us, it's easier than ever for them to get a good idea of

[4] https://leb.fbi.gov/articles/featured-articles/social-network-analysis-a-systematic-approach-for-investigating

where we are and who we associate with, without needing to send in operatives to figure it out.

So what do we do? Here are some easy-to-adopt ways to get started:

Instead of...	Try...
SMS, Meta Messenger, Discord, Gchat, Teams, etc.	Signal
Gmail, Outlook, Hotmail, Yahoo!, etc.	Tutanota, Protonmail
Google Docs, Microsoft Office 365	Cryptpad
Zoom, Google Meet, Teams	Jitsi
Apple Maps, Google Maps	OpenStreetMaps, Organic Maps
Google, Bing, Yahoo!	DuckDuckGo, SearXNG

As per usual, this isn't a comprehensive list but a place to begin.

Bringing It All Together

Relational Security helps to create cohesive and effective small groups. Together, in those small groups, you can identify Threat Models applicable to your work and organization, and implement methods—like Cybersecurity tips—to ensure that your network stays safe. Security Culture is the culture that we're co-creating as we do the work, and says as much about us as it does the threats we're countering.

Take some notes? Do some doodles? Have fun!

Further Reading

1) *Kill the Cop in Your Pocket.* https://www.anarsec.guide/posts/nophones/
   Makes the compelling argument about why NOT to bring your cell phone, and details the information gleaned from carrying it.

2) Morris, Courtney Desiree. *Why Misogynists Make Great Informants*. https://archive.org/details/WhyMisogynistsMakeGreatInformants
   Using the example of Brandon Darby and the Common Ground in New Orleans, discusses how sexism invites disruption of organizing spaces.

3) Neighborhood Anarchist Collective. *Activist Checklist (site).* https://activistchecklist.org/
   Various checklists that give easy-to-follow steps to think about when organizing, drawn from on-the-ground experiences from organizers.

4) Okun, Tema. *White Supremacy Culture.* https://www.whitesupremacyculture.info/
   A list of white supremacy culture traits that show up in organizations, and some antidotes to assist in ensuring that we don't perpetuate harm and exclusion in our organizing.

5) Umi, Ahjamu. *Movement Disagreements on Social Media Openly Serve the Police.* https://hoodcommunist.org/2020/05/14/movement-disagreements-on-social-media-openly-serve-the-police/

Reflections as to the impact of Social Media disputes on activism and organizing.

6) Williams, Kristian. *Profiles of Provocateurs.*
https://archive.org/details/ProfilesOfProvocateurs_197
Reviews profiles of different known informants and disruptors, and highlights traits that may indicate red flags/a need for additional scrutiny.

7) *Introduction to a Self Managed Life: a 13 hour & 28 minute presentation by FUTO software.*
https://wiki.futo.org/wiki/Introduction_to_a_Self_Managed_Life:_a_13_hour_%26_28_minute_presentation_by_FUTO_software
A hardcore guide to freedom from corporate tech overlords; not for the faint of heart.

8) Electronic Frontier Foundation Tools.
https://www.eff.org/pages/tools
Multiple links and resources that will help you stay safe with technology.

9) Biddle, Sam. *ICE Wants to Know if You're Posting Negative Things About It Online.* https://theintercept.com/2025/02/11/ice-immigration-social-media-surveillance/
This not only talks about what ICE is doing to try and figure out who potential activists are, but it reveals some of the technology the state uses to pin down activists.

Dedicated to Bean.