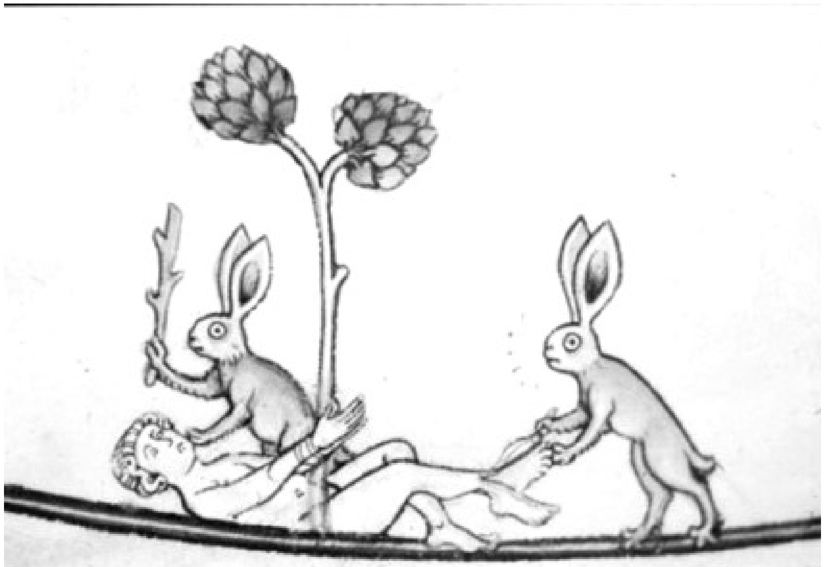
I want to have the kinds of security practices that allow me to be open while knowing that Ive assessed the risk I face and am taking smart steps to minimize it. Security culture should make openness more possible, not less.

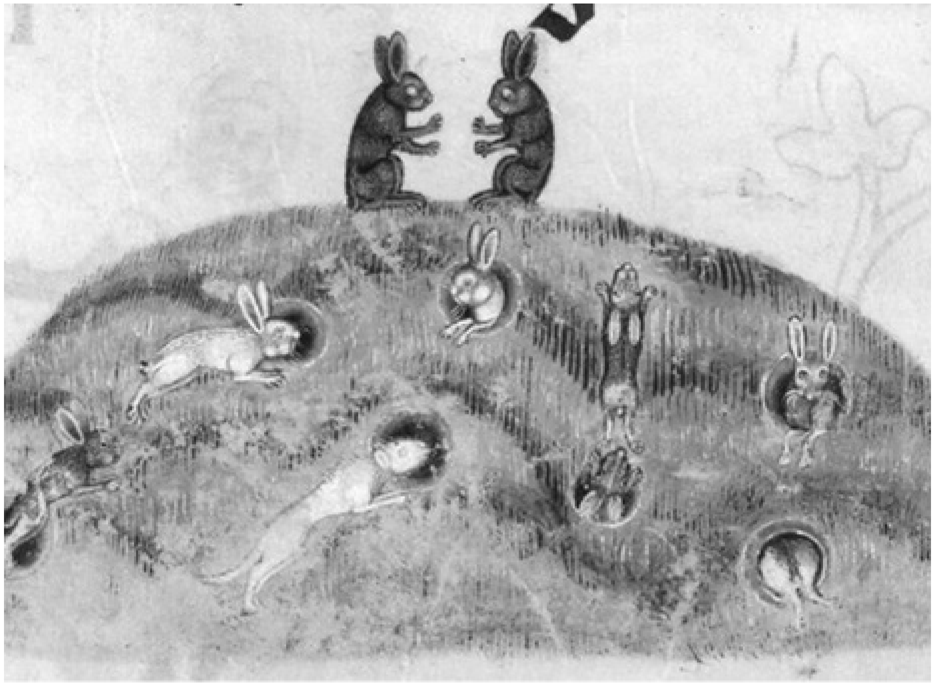
This proposal for security culture is based on reframing: on shifting our focus from fear to confidence, from risk aversion to courage, from isolation to connection, and from suspicion to trust.



This text is a short excerpt of a longer article. For the full text, visit North Shore Counter Info

Confidence. Courage. Connection. Trust.

A Short Introduction to Security Culture



(This short intro is made up of excerpts from a longer article. For the full text, visit north-shore.info)

When we talk about security culture, people tend to have one of two kinds of experiences. The first is of building walls and keeping people out, the second is of being excluded or mistrusted. Both of these come with negative feelings – fear and suspicion for the former and alienation and resentment for the latter. I would say that they are two sides of the same coin, two experiences of a security culture that isn't working well.

I want to be welcoming and open to new people in my organizing. I also want to protect myself as best I can from efforts to disrupt that organizing, especially from the state but also from bosses or the far-right. That means I want to have the kinds of security practices that allow me to be open while knowing that I've assessed the risk I face and am taking smart steps to minimize it. Security culture should make openness more possible, not less.

This proposal for security culture is based on reframing -- on shifting our focus from fear to confidence, from risk-aversion to courage, from isolation to connection, and from suspicion to trust.

Security culture refers to a set of practices developed to assess risks, control the flow of information through your networks, and to build solid organizing relationships. There are countless different possible security cultures, but the important thing is that they come from clear, explicit conversations about risk that are ongoing and respond to change.

One common objection people have to discussions of security culture in their organizing is: "I'm not doing anything illegal so I don't need to think about security."

strong, trusting relationship with a lot of capacity. A dashed line could mean some trust, and a dotted line means you don't know each other well. This collaborative process will reveal a lot about group dynamics and also show where there is work to be done in building more trust.

Flexible organising structures refer to the ability of our organising to adapt to reflect the needs of various kinds of activity. The key is to respect and legitimate individual initiative, by not for instance demanding that all activity pass through some sort of central body. This allows for certain projects to happen on a need-to-know basis even if other aspects of the organising are more open.

Finally, proactively addressing bad dynamics is just a good habit to have in general, but it's an important part of security culture. There are a lot of dynamics that erode trust and can make organizing harder. Bullying is one example. Another is oppressive behaviour rooted in patriarchy or white supremacy. Having clear politics about race, gender, and other oppressions as well as practices of addressing those issues head on can make it less likely that they will act as blind spots that undercovers can use to avoid scrutiny. But as well, bad dynamics in a group are often as disruptive as any undercover could be and are worth addressing in their own right.

(*For discussion of social media and tech security, as well as way more examples, see the full article!*)

mobilization? What level of trust do we need in each other for the kinds of things we want to do? It might be that we are at risk of undercover police infiltration, so knowing that we all are who we say we are could matter. We could also be concerned about infiltration by the far-right, in which case understanding each others politics and building trust gradually through slowly escalating actions could be key.

There are many different security culture practices that groups have experimented with and I'm not going to try to be exhaustive. Rather, I'd like to share a few that I and the people around me have had success with. These are ID checks, vouching, circles of trust, flexible organizing structures, and proactively addressing bad dynamics.

ID checks are for establishing that someone is who they say they are. This would look like taking a person out for coffee and, without advance warning, producing my ID and maybe a family photo or school yearbook. I would tell the person I wanted them to be able to trust I was I said I was, because I wanted us to be able to take riskier actions together. We then discussed what that person could show me.

Vouching is a practice for bringing new people into an existing group or organizing space. The first step is to have a clear basis for trust within your group. Whatever it is, vouching involves one or more people introducing a new person and stating explicitly that the person meets the basis for trust. Others present should explicitly accept or reject the vouch.

Circles of trust are mostly for informal networks and affinity-based organizing. It involves writing out the names of people in your network in a circle, and then drawing different kinds of lines between them to represent the kinds of relationships people have. A solid line could mean a

The choice to repress or to disrupt organizing belongs only to the state – it doesn't necessarily have very much to do with the actions being criminalized. Personally, I have a number of criminal convictions, have spent about a year in jail, two years on house arrest, and something like five years on various kinds of conditions. All of these convictions are for routine organizing tasks, like facilitating meetings and promoting demonstrations. The state chose to target them with conspiracy charges when it did because of large-scale policing and intelligence operations tied to summit protests and defending pipelines, even when my organizing was not linked to those events.

I don't say this to position myself as a victim – I want my organizing to be threatening to power, it makes sense to me that it would be targeted. We need to be aware that stories like mine are increasingly common and organize with forms of security that are adapted to this. Otherwise the only option is to restrict our own activities preemptively, to internalize that repression and integrate timidity and weakness into our work.

However, security culture is not only about resisting criminal charges. It's about preventing our activity from being disrupted. Criminal charges are a particular threat, but they're far from the only one. Some undercovers build up conspiracy charges, but others have changed passwords on websites and email addresses, directed buses to the wrong locations, stole medical supplies, spread harmful rumours to aggravate social conflict, and even attempted to entrap youth in a weird bomb plot. All of these police actions were immensely disruptive, without ever needing to rely on the power of the courts, and we will probably never have a full picture of their impact.

We might also be targeted by groups other than the state, for instance with civil lawsuits from bosses, doxxing and street violence by far-right groups, or harassment and brutality by private security. As well, even without negative consequences, simply losing the element of surprise when we need it could cause an otherwise well-planned action to fail. Security concerns are already integrated into much of the organizing we do. Building a security culture involves being explicit about assessment of risk beyond just specific actions and adopting clear practices designed to keep us safe and our actions effective across all the forms our organizing takes. Good security culture means doing this while emphasising strong connections, building trust, and feeling confident.

Here are a couple of general principles that underline security culture as I understand it.

The Two Nevers. “Never talk about your or someone else’s involvement in activity that risks being criminalized. Never talk about someone else’s interest in criminalized activity.” This is principle is inadequate, since we aren’t only concerned about criminal charges. But having a clear rule that is widely agreed on about not running your mouth about illegal stuff is a good idea no matter what space you’re in. This includes things we might feel are jokes.

Privilege face-to-face meetings. We build better trust, stronger relationships, and come to better decisions when we take the time to meet in person. For all the uses of electronic communication in your organizing, ask yourself if it’s replacing face-to-face meetings, and if it is, ask if it really needs to. Consider reducing your reliance on these things and begin trying to shift more conversations back to in person.

Repression is inevitable, or avoiding it at all costs isn’t worthwhile. Regardless of the struggle, if it’s taken far enough it will become a struggle against the police, those defenders of the world as it is. One way of preparing for repression is to centre police and prisons in our organizing from the beginning. In this, we can learn from anti-racist movements who almost always keep in mind the physical, racist violence of those institutions, even as they might choose to engage in a wider range of issues. We can take it a step further and incorporate practices of solidarity into our organizing.

Let’s look in more detail at what it means to assess risk. The important thing here is to do this openly and consistently, and to focus on how it makes possible the actions you think are effective and appropriate. It can be easy to get into a risk-averse mindset and self-police more than the state has the power to control us. Being explicit about risk can make it easier to focus on courage and possibility.

If you’re sitting down to plan a demo: Are you anticipating it to be calm and orderly? Or combative and uncontrollable? If the police try to block you, will you go along with it or will you try to push through? Are there actions you would be excited to see happen in the demo that risk being criminalized more than the act of taking the streets? Will your plans be jeopardized if you lose the element of surprise? Who do you not want to find out? How will you reach the people you want to reach without risking the wrong people catching wind?

Another example could be developing an antifascist organization. What kinds of questions about risk should we be asking even in the absence of planning any particular