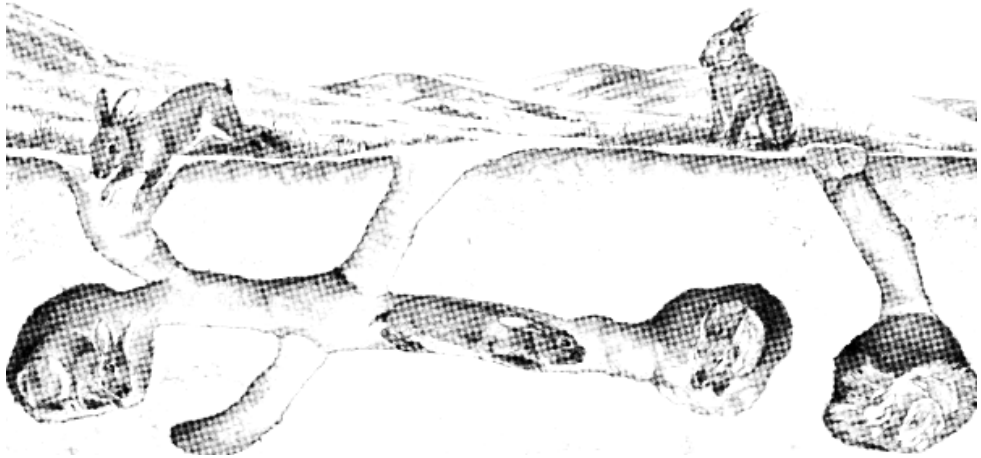
I want to have the kinds of security practices that allow me to be open while knowing that I've assessed the risk I face and am taking smart steps to minimize it. Security culture should make openness more possible, not less. This proposal for security culture is based on reframing: on shifting our focus from fear to confidence, from risk aversion to courage, from isolation to connection, and from suspicion to trust.

Confidence, Courage, Connection, Trust

A proposal for security culture



No Trace Project / No trace, no case. A collection of tools to help anarchists and other rebels **understand** the capabilities of their enemies, **undermine** surveillance efforts, and ultimately **act** without getting caught.

Depending on your context, possession of certain documents may be criminalized or attract unwanted attention—be careful about what zines you print and where you store them.

you take steps to protect your privacy like using private browsing. I recommend using Tor for any browsing or research. Corporate social media usually blocks Tor (reddit is an exception, and Twitter will let you Tor if you ask them), so if you are trying to have an anonymous account, an option is to use a VPN—a free one for use by anarchists and activists is available at riseup.net.

There is of course a lot more than can be done for tech security, but these three steps will already go a huge part of the way. A few years ago, we had a house raid hit us. The police captured something like fifteen laptops and phones, as well as many USBs and hard drives. Out of all this, only one laptop was not encrypted, since it had been left turned on. But out of the rest, not one piece of information was recovered. Similarly, our text and call history that could be accessed through our phone companies revealed nothing, since we use end-to-end encryption on services that protect meta data. We don't use social media or google to communicate, and so their searches of those platforms also gave them nothing. These tech security practices work when used correctly and consistently. There is a real difference in outcome when we use them and when we don't. They let us feel confident while connecting with others and contribute to building trust.

Thanks for reading! This text ended up longer than I expected, but I hope it's useful. I wrote this because there aren't a ton of good security culture resources out there, so I hope this will inspire people to have conversations about what kinds of practices are right for them, animated by a spirit of confidence, courage, connection, and trust. Let's us all keep our sights fixed on the world we are trying to create through our actions, instead of fearing the movements of our enemies. Good luck!

Confidence, Courage, Connection, Trust: A proposal for security culture

Original text in English

2019

north-shore.info/2019/11/05/confidence-courage-connection-trust-a-proposal-for-security-culture

Layout

No Trace Project

notrace.how/resources/#confidence

Finally, a word about **tech security**.[8] This topic is complex and it's easy to get bogged down on. However, there are a few simple steps we can take to greatly improve our data security. Here are three quick points.

One: Use end-to-end encryption unless you have a reason not to. This technology can be tricky, but at this point many applications exist that make it exactly as easy to use as conventional messaging. I recommend Signal, from Open Whisper Systems, though WhatsApp also uses similar encryption protocols, but without the metadata protection. The drawback is that these are not cross platform, while something like PGP, since it can work as just copy-pasteable blocks of text, can be used anywhere—any different email client, facebook and twitter, even text message. But it's harder to get started, and experience has shown that people aren't willing to put much work into their tech.

Two: Encrypt data where it is stored. Unless you have a reason not to, you should immediately encrypt your cellphone (Android has an option for this, many iphones are encrypted by default). For data stored on computers, external hard drives, USB keys, or online, I recommend VeraCrypt. It allows you to make encrypted 'boxes' that you throw your files into. This won't help you if your encryption is unlocked when your device is captured though. If you think you might be arrested, avoid traveling between places with your (encrypted) phone turned on. Consider getting an old-school alarm clock so you can turn your phones and computers off at night (which enables the encryption typically removed at startup), especially if you might be at risk of a house raid. Make encrypted backups of your data and store it somewhere else.

Three: Hide your online identity whenever possible. Your IP address is visible to every website or service you use and links your activity together in the eyes of your service provider and the state, even if

[8] *N.T.P. note:* For more tech security tips, see our Threat Library.[9]

[9] https://notrace.how/threat-library/mitigations/digital-best-practices.html

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.

It makes sense to feel fear—the state is very powerful, repression is common, and it has the power to crush us and all our projects. But I don't want to stay in that fear, and with accurate information and good plans we can begin to transform fear into **confidence**, knowing we have security practices that are up to the risk we face. In fact, without transforming fear, it's hard to imagine how we could manage to take action at all in face of the power of our enemies.

I don't want to be risk-averse. I want to decide on my actions based on effectiveness, appropriateness, my analysis, and my ethics. Good security culture lays the groundwork for us to show **courage** in our tactics collectively, since we know we can handle the risk. When we don't transform risk-aversion, we self-police and stay narrowly in the space for symbolic opposition that is provided to us.

Repression functions by isolating people. I don't want to contribute to isolation through the things I do to keep myself and my friends safe. I want a security culture rooted in deepening our **connection**

with each other. When we don't transform isolation, organizing can feel no different than work and we don't build the kinds of relationships that truly transform us, such that we can begin to feel the world we wish to create.

I don't want to feel suspicion when I meet people, that's toxic and erodes the spaces of struggle we create. Rather than feel suspicious of someone, I want to ask myself "what would it take for me to **trust** this person?" I want to go towards people and try to transform suspicion into trust.

I would like to offer a definition of security culture to frame this conversation. **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. In the following example, the ongoing conversation about risk reacts to changes in our actions and in how we are being targeted. The various security culture practices mentioned will be explained further down.

> In a pipeline campaign where I live, we wanted to emphasize mass direct actions targeting oil infrastructure. We decided that our risk for the early stages of that campaign as we focused on outreach and research was very slight and that we could safely involve many people in that work and share information about it openly on any platform. As we began planning symbolic protest actions, this consideration didn't significantly change, but when we began planning things like blocking roads or picketing a police station, the element of surprise became a larger consideration. Regardless of possible criminal charges, our actions would simply be less effective if they were known in advance. So we stopped using public or easily surveilled means to communicate and began asking that people only share details to trusted individuals who intended to participate.
>
> Soon after this phase of the campaign began, a national-level policing apparatus called a Joint Intelligence Group (JIG) came together around defending pipelines, involving many levels of

of their ability to reach their base. This can be a disaster if we are over dependant on these companies. Ask yourselves what you would do if all of your pages and accounts dissappeared tonight—how would you organize tomorrow?

There is also the issue of *surveillance*, which shouldn't be controversial. Everything that is typed into Facebook is saved forever in a database that police can access any time. Facebook software (like Google and others) tracks you and spies on your device, information that is also available to security and intelligence agencies. This is not a theory, it has been proven over and over again, and cases against activists relying on such information have only become more common across Europe and North America in recent years.

My **proposal for social media** is as follows. Privilege in person meetings and have them regularly if possible, so the next meetup is already set in case online communication is disrupted. When we're using social media, let's ask ourselves if it's really necessary and see if we can shift that conversation to another platform. I would encourage you to think of social media as a megaphone, a way of amplifying your voice, and not as a living room, for discussing and getting to know people. Use it to promote, to announce, to disseminate, but move conversations elsewhere. In my own organizing, we delete almost all comments from pages we manage and shift most messages to other platforms as soon as we receive them. We use shared accounts wherever possible and reduce our reliance on accounts tied to personal information. Perhaps you don't want to go this far, perhaps you want to go further, but this is one way of making use of social media's strengths while avoiding its massive drawbacks.

A transition in our use of social media can happen gradually, looking critically at our use of it and shifting these uses firstly to in person meetings and secondarily to other platforms, piece by piece. It took a long time for so much of our lives to be captured by these disgusting companies, and it might take us a while to build new organizing habits and cultures that are resistant to them.

In practice though, such objections to security culture come up most these days around the use of social media, of which Facebook remains the most common. To that end, I would like to offer a few **critiques of Facebook organizing** and offer a proposal for how large organizations that depend on it could respond.

A crucial point is that corporate social media *reduces the field of possibility* for organizing. Since it's about as private as organizing in the lobby of a police station and at this point almost everyone knows it, there are stark limits to what can safely be discussed there. Which means if we are dependant on Facebook as our primary organizing space, the limits of what can be thought or planned are taken on as our own. This kind of preventive disarmament is a real position of weakness.

Such platforms are also vulnerable to being *swamped by hostile reactions*. We can't control how our actions will be received, and sometimes things we do will be unpopular—we are afterall seeking a world without capitalism that is organized on a radically different basis. The online aftershock from an unpopular action can be destabilizing. In a recent antifascist mobilization in my town, the far-right and mainstream media successfully provoked a backlash against antifascists that flooded social media with threats and anger. Antifascists were heavily dependant on Facebook for their organizing and so were presented with a choice: either stay offline and avoid the backlash but be isolated from your comrades, or go online and talk with people, but have your conversations dominated by stress and hostility. This dynamic makes organizing much less resilient and means our work can essentially be disrupted by bad press.

An extension of this is the *corporate control of the platforms*. Facebook is an enormous, rich corporation whose interests are utterly opposed to ours—what's good for us is bad for them. If we depend on their infrastructure, they have the discretion to shut us down at any time, for any reason. Companies like this are very susceptible to public pressure and we don't have to think hard to find examples of projects that became unpopular and lost their pages, and along with it most

> police and intelligence services. JIGs and configurations like them are a specific threat to struggles of all kinds, since they aim vast resources directly at disrupting organizing. So even though our actions didn't change, we revisited our conversation about risk and decided to insulate the organizers of actions from possible conspiracy charges by doing the planning in a small, opaque group. We could invite people to participate who we trusted, and we might take steps to build up that trust, like doing identity checks of each other. But we would no longer plan actions openly in the larger network of people interested in the education and outreach work. This shift meant that when we moved on to shutting down critical infrastructure, we just had to scale up from this organizing node we had formed and encourage other crews to organize similarly, coordinating through a meeting of representatives from vouched groups to take on different roles.

(Of course, this organizing model, like all such models, comes with drawbacks as well as strengths. It's not my intention in this text to advocate for one particular way of organizing, though inevitably I have more experience with some than with others.)

Before digging more into specific ideas and practices, I want to speak to a common objection people have to discussions of security culture in their organizing: "I'm not doing anything illegal so I don't need to think about security." This could come up in a more specific way, like "I'm not discussing anything sensitive, so I don't need to worry about it being surveilled," or "I'm not usually stopped at the border, so I don't need to worry about the stacks of anarchist journals in my car," but the underlying objection is the same.

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 that the state chose to target with repression for its own reasons. I was sentenced to eight months in jail for facilitating meetings and for writing and distrib-

uting a callout for a march in the context of a big summit; some years later, I was sentenced to a year for distributing a leaflet announcing a march and then being in attendance at the march. In both of these cases, there was property destruction during the demonstration, but I was never accused of it. Rather, the state chose to use conspiracy charges to target people doing visible, routine organizing of the kind I have done many times. Similar dynamics have played out in other conspiracy cases in both the US and Canada, my experience was not exceptional.

I don't tell these stories 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. The important part is that the state chose to criminalize leafleting and facilitating meetings in order to intimidate or to make an example. Even if this kind of repression were to occur only 1% of the time (though it seems somewhat more common), we need to be aware of it and organize with forms of security that are adapted to it, 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.

During the big summit where I caught conspiracy charges, only two of the JIG's 16 undercovers were involved in the case. Other undercovers 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.

in our scenes for people to be made uncomfortable by patriarchal behaviour from men. Sometimes people will develop suspicion towards those making them uncomfortable in those ways, and this is understandable, but it's a mistake to begin looking for infiltrators when there is sexism right before our eyes. Destructive behaviour is worth dealing with in its own right, and if it helps us avoid informants like Darby too, all the better.

A note on formal, **mass-membership organizations**. Such kinds of organizing are often very resistant to conversations about security culture, since these discourses are most common in forms of organizing that look different than what they aspire to. Security culture can sound like a more general critique of their organizing than a proposal for how to strengthen it. Some of the practices above might not apply to formal, mass-membership organizations, but I would argue that all the general principles do. In fact, I think if such organizations look closely at how they operate, they will see that security practices already exist.

For instance, in branches of the IWW, it's not uncommon to attempt to keep workplace organizing drives secret. People involved in supporting the shop floor organizers might use code names with those not directly involved, or might make public only general information. As well, it's common for such organizations to strike smaller committees to take on specific tasks, like organizing a demonstration, and their conversations might not be open to those not involved, or they might communicate through different channels, for instance avoiding large mailing lists or social media.

All I would suggest is that explicit conversations about risk and security be incorporated into the different kinds of work such organizations take on, since they have different needs. Empowering committees to decide their own security practices and basis of unity is a great step, as is welcoming individual initiatives by members associating on the basis of affinity, meaning the organising structure is flexible enough to accommodate different ways of organising for different kinds of activity.

subculture for any amount of time won't have any trouble listing bad dynamics.

Like I said above when talking about complex and sensitve issues related to ID checks, our difficulty in dealing with bad dynamics and issues of oppression in our scenes creates a blind spot that police and intelligence agencies are increasingly aware of. I mentioned the cop who pretended to be a survivor to worm her way into peoples' lives (she was even brought in as a roommate to someone's house). Another undercover experience involved a cop who was a middle-aged brown guy who, when people would talk about how he made them uncomfortable (notably for breaching the Two Nevers), he was able to deflect concerns by claiming they were being racist towards him. He found a group of anti-racist activists in a different community from the ones he was most targeting to back him, and he successfully resisted multiple efforts to expel him from organizing spaces. Ultimately, he went on to testify in a case that sent six people to jail. He doubtless experienced racism in our scenes, and this and his cynical manipulation of anti-racism should also cause us to examine the weakness of our anti-racist politic. Having clear politics about race, gender, and other oppressions (meaning that you are comfortable saying in detail what your analysis is around them and why) as well as practices of addressing those issues head on when they come up can make it less likely that plays like this will work.

There are many reasons why someone might be untrustworthy and many kinds of predatory behaviour that aren't being a secret cop. We don't usually need to be asking ourselves if people are cops. An example is Brandon Darby. In the text "Why Misogynists Make Great Informants",[6] the authors make the point that people should have tried to do more to deal with Darby's awful sexist behaviour before he ever began cooperating with the FBI,[7] ultimately entrapping several people. He is an extreme example, but it's very common

[6] https://notrace.how/resources/#why-misogynists-make-great-informants

[7] *N.T.P. note:* Federal Bureau of Investigation, the main federal law enforcement agency and domestic intelligence service in the United States.

We already saw that often maintaining the element of surprise is an important security consideration—an example in our area is organizing prison demos to support people who are locked up: organizing them quietly means we can have freedom of movement and action for a period of time before the police are able to mount a response. Or consider an IWW[1] chapter trying to do a reclaim your pay campaign against a boss—they will need to take steps to protect themselves from civil lawsuits or from being targeted by private security. Or consider the work antifascists do to identify the far-right—they need to be mindful to avoid having their own personal information become public and targets of violence in the street. There are also private security companies that are increasingly hired to defend private interests in ways that the police can't or won't, which has come up repeatedly around indigenous-led land defense struggles in recent years.

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. These points are somewhat well-known, but also quite inadequate. Their most basic framing is "Never talk about your or someone else's involvement in illegal activity. Never talk about someone else's interest in illegal activity."

The most obvious inadequacy is that a lot of what we do doesn't involve obviously illegal stuff. We could reframe the Two Nevers like this: "Never talk about your or someone else's involvement in

[1] *No Trace Project (N.T.P.) note:* Industrial Workers of the World, an international labor union founded in the United States in 1905.

activity that risks being criminalized. Never talk about someone else's interest in criminalized activity."

This is still 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—loose talk about fighting cops or attacking property might not seem harmless when entered into a snitch's notes.

One of the most common reasons people become suspicious of someone is if that person is trying to take people off to one side to discuss illegal tactics. Rather than saying, "this person is a cop trying to entrap me", we can reframe and say, "I need to clarify my understanding of security culture with this person if we are going to work together". The rephrased version of the Two Nevers can be one simple way of doing that. It also reminds us to not try to figure out or speculate about who pulled off actions happening anonymously around us—that's the cops' job. If others ask about anonymous illegal actions, you can gently remind them the action was done anonymously, it doesn't matter who did it, and it speaks for itself.

(A less recognized form of bad security culture is how callouts around security culture can reinforce negative power dynamics. We should absolutely talk to each other about interactions we have security concerns about, but this should always be mutual and done privately when possible—describe what you heard, present your idea of security culture, ask if they think that's a reasonable boundary, be willing to hear them disagree. The goal is to build shared understandings to widen the range of organizing we can engage in together, not shut people down or make them feel ashamed (or to make ourselves seem more hardcore). An extreme form of this is snitch-jacketing, where people are falsely called a snitch, which can have huge consequences in peoples lives and were a part of eroding revolutionary movements in the 70's, but a smaller example could be a more 'experienced' person shutting down others in front of a

of informal, affinity-based organizing is one that has developed to respond specifically to this need. In an informal (as in, without a fixed form) network, individuals communicate about their ideas and intentions, and affinity groups form around a specific project or around a shared desire to intervene on a common basis. The strength here is that it's very easy to initiate projects of various risk levels with security culture practices adapted to each. As well, there is an element of need-to-know incorporated automatically, in that only those involved in the organizing know its details or who is involved, unless those people decide otherwise.

Similar flexibility can be incorporated into other organizing models. 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 can happen as an unspoken norm in loosely structured activist groups as well, not just as a rule in groups with fixed decision-making process). As well, respect for voluntary association, meaning it's seen as normal for people to work together in smaller, chosen groups alongside larger, more open structures. In a formal way, this can look like the use of committees or working groups that have the ability to set their own standard for participation. It can also just look like being open to elements of affinity-based organizing as described above, or by being explicit about what kinds of information are need-to-know.

Finally, **proactively addressing bad dynamics** is just a good habit to have in general, but it's so important to security that it should be emphasized in every conversation about 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. Yet another is centralizing contacts and resources, which means only certain people can lead projects. Others might be shit talk, boasting, or poor security practices like violating the Two Nevers by asking about people's involvement in criminalized activity. Anyone who has been involved in an activist

to take a vouch on someone's word without details about specific activities.

Circles of trust are mostly for informal networks and affinity-based organizing (which, to be clear, is most of my organizing experience). 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 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.[5]

It might show that only one person has strong relationships with everyone and that other peoples' relationships are less solid. This means there is work to do in making that more balanced, which makes groups more resilient (in case that one person gets arrested or even just gets sick or burns out) and also more egalitarian, since the ability to initiate projects is tied to the amount of trust people have in the person initiating them. The exercise might also reveal that some people are trusted by no one. This shows that work needs to be done to get to know that person better and see if trust can be built there.

Oftentimes, infiltrators will first approach one community, then use the contacts from there to name drop their way into a different scene. Vouching and circles of trust are great defenses against this. But more than finding hostile people, circles of trust encourages us to build strength in our networks by trying to turn as many of those dashed lines solid as we can.

Flexible organising structures refer to the ability of our organising to adapt to reflect the needs of various kinds of activity. The practice

[5] *N.T.P. note:* After carrying out this exercise, we advise you to immediately destroy the support used for the exercise so that the cops don't come across it one day.

group for talking about actions they found inspiring or for who they are talking to.)

Another point is to **privilege face-to-face meetings**. Regardless of the platform or how secure or insecure it is, we build better trust, stronger relationships, and come to better decisions when we take the time to meet in person. When electronic means of communication replace the face-to-face, our conversations are easier to surveil, misunderstandings come up more often, and they can be disrupted by decisions or problems at far-away companies. 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. (More on tech stuff in a bit…)

An objection to this is that many people have social anxiety and prefer to communicate using their devices; another is that physically traveling places is a barrier for some. Like other sensitive issues that come up around security culture, I encourage you to deal with them head on and dig into other ways of accommodating those needs while still attempting to prioritize meeting in person. After all, these technologies are very new and people with disabilities of all kinds have a long history of finding each other to organise around the issues that effect them.

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. If we take as a starting point that we will avoid repression at all costs, then we will only use forms of struggle approved of by the police, which makes it pretty much impossible to build collective power capable of transformative change. If we don't accept these limitations, then we need to be prepared to face repression.

One way of preparing 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. The advantage is we already build up a politic that isn't shocked by police violence and that is realistic about prison. We can take it a step further and incorporate practices of solidarity into our organizing. We might be organizing in a labour space—look at labour struggles elsewhere and find practical acts of solidarity to do towards those facing repression. We might be organizing around queer stuff—find and support queer prisoners, this way you'll know how to navigate prisons in your area if and when you need that knowledge. If you're interesting in environmental struggles and land defense, there are land defenders in jail, fighting charges, and facing the physical violence of the state all across the continent—incorporating practices of solidarity with them into your work can give some powerful inspiration for creative, courageous resistance.

A further benefit is that you are more likely to receive solidarity in turn, since prisons are a great unifying force, linking all the various struggles against domination and oppression. Being in a resistance culture that shows active solidarity in the face of repression can go a long way towards keeping yourselves safer. And again—we combat fear with accurate information. The more we know about how police and prisons work, the more we can shift from fear to preparation and confidence.

With these points in mind, 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, think about tone. 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

Vouching is a practice for bringing new people into an existing group or organizing space. Like our other practices, it is best when it is explicit and done consistently. The first step is to have a clear basis for trust within your group. Perhaps your basis is just that someone has politics compatible with yours and is reliable. Perhaps you need to know people are who they say they are, that they stay solid under pressure, that they have certain kinds of organizing experience, and are comfortable with certain kinds of action. 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. Being explicit in this way avoids some of the risk of implicitly trusting people for superficial reasons, like for fitting certain subcultural norms or being read as having a certain identity.

Here's an example of a vouch:

> "I have known this person for five years. During that time, we've worked closely together on public projects and I trust them to have my back when things get tough. I went for dinner at their dad's house one time and I've picked them up from work frequently."

Here's another example:

> "I met this person last year at a public event about climate change and we've seen each other around at environmental events regularly since. We've talked a lot about the issues and I like them a lot. I know they're looking to gain some experience organizing actions and I think they'd be a good fit with us."

An exception to being explicit about why you trust someone is that you shouldn't breach the Two Nevers. If you are organizing clandestine actions, bringing in new people or introducing crews to each other is tricky, and the concerns are different. Vouching is still a good idea, but you also don't want to increase risk for anyone by talking about past actions. Since there needs to be a strong basis of trust to be doing those actions in the first place, it could be possible

to take riskier actions together. We then discussed what that person could show me. Sometimes this involved phone calls to work or to family members on speaker phone, so I could hear the person on the other end provide details of someone's life or employment. Other times ID was enough. Sometimes we would go back to each others' apartments. The idea was to be as mutual as possible (which is hard since in practice someone is initiating it) and to keep the focus on building trust.

It's not useful to incorporate ID checks with people you don't trust or with whom you won't feel comfortable taking riskier actions regardless of how they go. This is not about finding cops, it's about deepening trust and confidence. Checking each other in this way should be a sign of respect.

There are a lot of factors that can come into play to make this less straight forward. For instance, people who immigrated to the country might not have family nearby or have the same kinds of documentation. Queer and trans people often don't use the names on their documents and might not be comfortable sharing legal names or old pictures. However, these are things to take into account and to adapt to, not reasons to skip getting to know someone. One undercover cop in my area claimed to be escaping an abusive relationship and used our politics around supporting survivors to shut down any conversation about her past. Our discomfort around complex and sensitive issues creates blind spots that people who wish us harm can walk into—we need to be brave and find ways of addressing this complexity, not avoid it.

One friend with experience doing this added there might be moments where its OK to be less mutual, where you might not want to give people as much control over what proof looks like. They also emphasised that this wont necessarily help with snitches (as opposed to undercovers) who are who they say they are but have bad motives. You also need to have a clear sense in advance of what you will do if someone can't or won't go along, or if you turn up something that requires you to rethink your trust in the person.

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? This could be as simple as stickering or could be spraypainting or breaking windows. 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? Communicating clearly about the tone of an action can help others come with autonomous plans that are suitable.

It's important to avoid complacency or taking too much for granted. Here's an example from 2018:

> The organizers of an anarchist bookfair decided to call a night demo for after the event. They were putting much more energy into other aspects of the day and were complacent about risk at the demo, because they'd organized a hundred demos before. However, the demo ended up being much more combative than others and a lot of property destruction occurred—they hadn't assessed risk explicitly and hadn't taken the time to consider it in an ongoing way as the start time got closer. As well, they hadn't taken into account that a JIG focused on a G7 summit in a different province that summer might have meant there were additional police resources aimed at them during this period. This meant that their security practices in the lead up were not adapted to the level of risk the action ended up having, and all of the bookfair organizers were charged with conspiracy.

This is an extreme example, but there will always be unexpected things that happen, and that's generally a good thing, since we can't fully plan our way to an insurrectional situation. Staying active in our risk assessment can mean we are less likely to be caught by surprise, and having strong security culture practices that we always use can reduce the harm when situations like this occur. In this case, good data security, a culture of non-cooperation with police, active and persistent solidarity, effective masking, and a refusal to give up or submit meant that this unexpected situation was much less harmful

than it could have been and people got through it with their heads up.

Another example could be developing a mass organization, say an antifascist organization. What kinds of questions about risk should we be asking even in the absence of planning any particular 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 infiltrattion, 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. Our principle around face-to-face organizing above online activities will likely make it easier to achieve both of these goals.

If the intention is to build towards street action, then a part of the security conversation could be about discipline and how to plan. What are our expectations of each other in tense situations? It's hard to honour expectations when expectation are vague, and it's easier to act smart when have a clear plan for what you're there to do and can tell if it's working or not. Building good organizing habits about what to consider as a group has major consequences for safety in the streets—it's not the same as security culture, but the conversations are closely related. For instance, risks around antifascist mobilizations might include ending up outnumbered, getting ambushed or separated, being followed or being identified by the far-right or by police, or suffering unnecessary injuries or arrests.

Some organizing practices for mobilizations that address risk include:

- Cut-off numbers: a number of participants below which the action is either canceled or shifts to a lower intensity back-up plan.
- Exit strategies: when will you leave, how do you tell people, where do you separate, how do you avoid being followed, how do you check people are home safe?

- Meet-up points: gathering as a group before heading together to an action site.
- Appropriate street tactics: positioning in two lines with complementary roles, for instance.
- Clear communication practices: how will you communicate in the streets, will you bring phones,[2] what names will you use for each other?
- Scheduled check-ins: how will you check in with each other after leaving to make sure everyone is safe, getting together soon after to debrief an offer support.

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.[3] In the pipeline campaign I described above, when we wanted to shift towards more intense direct actions, we needed to deepen the trust and collective strength among those we'd been organizing with. Because we were talking about risk regularly, we understood that the security practices we had used for protests, rallies, short-term occupations, and educational events weren't appropriate for this. Since we were concerned about infiltrators, we decided to ID check each other. 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

[2] *N.T.P. note:* We advise against bringing a phone to a demonstration where there is a risk of arrest, unless it is a phone purchased anonymously for the occasion, and equipped with a SIM card also purchased anonymously for the occasion.

[3] *N.T.P. note:* Techniques other than ID checks can be used to verify that someone is who they say they are. For more information, see our Threat Library.[4]

[4] https://notrace.how/threat-library/mitigations/background-checks.html