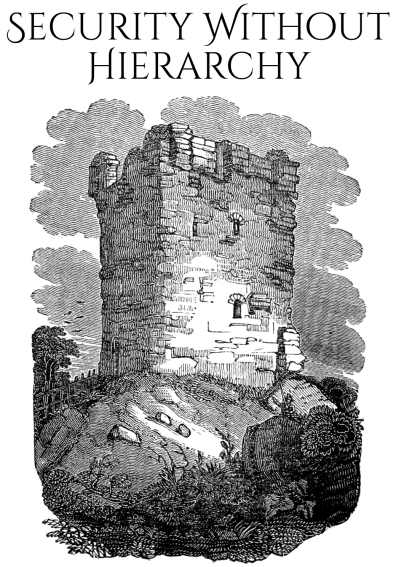
Scrappy Capy Distro
Security Without Hierarchy
3 August 2023

Retrieved on 6 January 2024 from en.scrappycapydistro.info.
Zine:
en.scrappycapydistro.info/zines/security-without-hierarchy

theanarchistlibrary.org

Security Without Hierarchy

Scrappy Capy Distro



3 August 2023

Contents

dence, Courage, Connection, Trust: a proposal for security culture by an anonymous comrade is probably the most useful modern text on security culture, and it describes approaches for taking a positive rather than negative approach to security. *Stop Huntin' Sheep: A Guide to Creating Safer Networks* by Sirens of a Violent Storm offers practical advice on how to deal with infiltrators so that we can stop turning security against ourselves. *Secrets and Lies* by Ungrateful Hyenas Editions is similar to this text in that it describes pathological applications of security culture, though it does so from a different angle.

preferences, protecting the coherence of an organization, or repelling those who might challenge informal power structures. Like many anarchist methods, they can be pathologically applied, misused, and perverted to serve authoritarian and malicious ends. This isn't an argument against security culture. It's acknowledging the ways that we end up having to wield power—even just a bit, even nobly—to protect ourselves. Power and hierarchy can never be fully abolished, and we will perpetually fight against them no matter how utopian our world becomes. Maybe this shouldn't have been called *Security Without Hierarchy* but instead *Hierarchy-Conscious Security*, though that doesn't have quite the same ring to it.

Now, where do we go from here?

We're going to have security culture, but whether or not it's predominantly beneficial or predominantly pathological depends on how we approach it. If we're intentional about building open, mutual relationships, we might end up with a healthier security culture that contributes to a healthier scene. If we stick with tradition or aren't able to counter those who use security as a weapon, how we organize might be anarchist in name only. There's no approach that is guaranteed to work, and I can't pretend to be able to say that there's solutions that work everywhere or even that these proposals work at all. I've just experienced harmful dynamics driven by security or at least that use security as their justification. Maybe by naming them and describing how they function, we can all find ways to counter these trends so that we can forge new and strong connections we can use in the fight to end coercion.

Further Reading

If you've seen some of these patterns, and if you want to find ways to understand them better or even address them, there's a few other texts you might want to consider. *Confi-*

Power can creep into every part of how we organize, take root, and create hierarchies. Security culture is one such case, and through both accident and malice, we can create new hierarchies and exacerbate existing ones. This zine reflects on the ways security culture can lead to harmful organizational patterns and structures within our collectives and movements, and it offers some possible methods for addressing it.

This is based on a series of talks with the same title given at anarchist convergences in the summer of '23 in Stockholm, Ljubljana, and St. Imier. Following each talk, the content of the zine and future talks were improved by the discussions with others in the rooms and later in the nooks and crannies of the venues. The words on these pages are not solely my own because knowledge isn't incepted out of nothing but rather synthesized from our past experiences and interactions with others. We learn together, not alone.

Discussions of security culture tend focus on ways to keep out infiltrators or avoid surveillance. We have plans for how to not be recorded or leave a trail of evidence as we take action, and we have our rituals for keeping infiltrators at bay or rooting them out when they turn up. These discussions in many cases are less grounded in the material realities of repression but rather more in the pitting of different dogmatic approaches to security against each other. When security culture actually is more broadly dicussed, it tends to revolve around the question "are we doing enough?" We reach for zines or hold workshops that are instructional on how to do "more security." More security, fewer phones. More secrecy, fewer leaks. There is a lack of reflection on how the current application of security might be damaging to individuals or the movement as a whole.

Along with all the beneficial ways we apply security culture, there are pathological applications. Sometimes this happens on accident through many well-meaning actions whose sum leads us to undesirable behavior. Other times security culture is weaponized by the Horrible Creatures[1] who inhabit our scenes and don't aim to abolish power over others but instead climb the social ladder to claim the highest position for themselves, and we also need to account for this in how we construct our norms.

What follows is a critical discussion of the ways we pathologically apply security culture. The very thing that is intended to protect us from external harms can be the instrument of harms and disruption itself. When we're not careful, we can accidentally reinforce existing hierarchies or even create new ones.

[1] A reference to an essay of the same title, which I can whole-heartedly recommend.

Importantly, progressively smaller circles are nested within *within* the larger circles. These smaller collectives down to affinity groups are not isolated from within the broader milieu, but rather are embedded in it. This embedding is important because it allows us to mediate the flow between larger and smaller circles, from areas of lower trust to higher trust. Deepening relations allows us to deepen trust, and this deepened trust is a necessary criteria for taking radical action. Isolated affinity groups that aren't embedded within a broader scene will eventually die out, and without pulling in new comrades, they will not reproduce. This is a dead-end for anarchism.

Instead of restricting the flow of information and connection, we want to encourage overlap between circles. We want to facilitate connection. This doesn't mean giving up control, but instead guiding growth. We want comrades to be mutually involved and develop both deep and broad connections.

One note on this method is that in smaller cities with a limited scene, and especially in small town organizing, there might simply not be enough of a scene for this strategy to work. The lack of anonymity of a big city means everyone knows a little bit what everyone is up to, and two insurrectos who propose conflictuality as a strategy might be "known" to all as the ones who carried out some direct action simply because they are the only ones who might conceivably even do it. I unfortunately cannot offer meaningful advice on how to model this kind of security as I have insufficient experience in such contexts. Perhaps then I'll leave this as an exercise to the reader.

Closing Words

Security culture is a necessity for organizing, but when we're not careful, we can create hierarchies. This often comes from trying to control the flow of information or access to resources, but it can also come from reinforcing in-group

ing others to a shared space or hosting events whose purpose is facilitating the building of new social connections.

Proposal #5: Move Beyond "Us and Them"

Related to the critical evaluation of risk, and perhaps both the most practical and important of all, is to move beyond the idea of there being a clear "us" and "them." Such a false dichotomy tends to mean drawing a line where people on the same side are assumed to be safer and more trustworthy and people on the other side less so. This is a poor heuristic. Of course, not everyone has such strict lines. Within the sphere of "us" and "them" there are varying levels of trust and assumed safety, but broadly speaking trust gets over or under assumed depending on where someone falls on that line. One way to conceptualize thinking in this manner of trust is that it is like an egg. There's a hard outer shell, that keeps the bad things out, but once something gets in, it can scramble the insides quite easily.

A more useful way of framing security to imagine concentric and overlapping circles. Large circles that include more individuals are for organizing mass events: demonstrations, workplace unions, or even just events like info evenings or film screenings. These events are low-risk, so we don't need to work about heavy security norms. These large circles might overlap where people who attend book readings also show up to cook in the community kitchens. There are also progressively smaller circles as one moves from minimally repressed activities to heavily repressed ones. The circles get smaller *because* we need to have already established high trust which takes time thus limiting the number of people who could conceivably be involved. Larger circles might have more overlap with other large circles, but because of the higher security needed, smaller circles might intentionally *not* overlap (but sometimes they will).

On Security Culture Itself

What are we talking about when we say security culture? There are many ways to define it, and some make a point to emphasize the most positive elements, but for now it's more useful to think about how people *actually* use the term rather than how they *should* use it. A definition that is broad enough to be applicable to both the beneficial and pathological implementations is: security culture is the practices and norms that are claimed to protect a group from repression or (external) disruption.

In 2004, CrimethInc. published the still-relevant text *What Is Security Culture?*. The first of their theses on security culture was:

> 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.

Regardless of how it was intended or the extent to which it captured practices in the preceding years, it has become somewhat of an edict in anarchist circles. This quote recurs in anarchist texts, discussions both online and off, and even in memes that get passed around. Or perhaps this quote is popular because modern practitioners of security culture find that it mirrors how they approach the topic. In any case, security culture is often seen as *controlling the flow of information.*

This approach makes sense because we are often trying to keep confidential information from being exposed to enemies. A spontaneous demonstration requires that police are unaware of its existence until after it starts if it is to be successful. The identities of the individuals who took part in a direct action must remain indefinitely hidden.[2]

[2] Or at the very least until that statute of limitations for any criminalized activity has passed.

We are, however, always dealing with varying degrees of uncertainty. Because we don't have perfect knowledge of those around us, we can't be absolutely sure that it is safe to tell them anything. Someone might be an opportunist and will rat out their "comrades" at the first chance to benefit from doing so. A comrades who is 100% solid today might change their ideals. But also, we cannot be sure who—including ourselves—will crack under coercion, tortuous or otherwise. Or, we don't know who is a straight-up police infiltrator. This isn't even including the ways information accidentally leaks out either through covertly recorded conversations or intercepted electronic communications. We preemptively cut the flow outward so that leaks don't spring up further down the line. But, we will never know for certain who is "safe" and who is "unsafe."

Controlling information flows is a specific case of the general phenomenon of security culture being used to *control access toresources*. We fear the intelligence gained by an infiltrator, but we also fear the damage done by a police saboteur, a wrecker who is out to derail our projects, or an abuser who causes great harms and breaks our spirits. We might deny access to even casual meetings or social events to people based on them not fulfilling some criteria of trustworthiness or assumed safety. We might not let unknown collectives use the spaces we control, and we might deny admission in to a collective or working group based on someone being too "unfamiliar." This suspicion of infiltrators or abusers creates a culture of fear where groups turn inwards and hold people at arm's length.

The result of this is an increased threshold of trust required to engage in even the most basic of organizing. Security culture in these cases becomes less about analyzing which information should remain privileged or which activities could lead to repression, and instead this mistrust leads to restricting *all* information, activities, and resources.

these conversations can't or won't happen, chances are you are part of a project with strong informal hierarchies, and you might be better off leaving to start your own.

As noted before, many people's pursuit of safety is a trauma response, and working through such trauma can lead to a healthier security culture. There is no replacement for therapy—professional or autonomously organized—but the threats of repression can be demystified by having these intentional discussions of security, and this goes hand in hand with critically evaluating risk. Instead of a vague spook of the State looming over our every action, we can outline not just what threats we face but what we can do about it *together* to create genuine security for everyone.

Having these discussions can also be educational in a general sense. This cuts into the authority the techies and security enthusiasts have with regards to the security practices of a group, and it allows us to build up shared knowledge so that we can reason through decisions together instead of relying on the words of a single individual.

Proposal #4: Call Out Protectionism

As part of the intentional discussions, but also every time it happens, we need to call out the ways security culture becomes protectionism. This is often made difficult if there is already a culture of exclusion that permits the accentuation of in-group preferences. Countering protectionism under the name of security culture starts with changing the underlying social relations that pathological security culture justifies. To change a culture is no small task, but it's also something we can all start by being more open with how we organize in a general sense. When a security practice starts to veer into protectionism or in-group preference over genuine security, we need to pause and reflect on it. Usually specific and intentional interventions are necessary, and examples of these can be intentionally invit-

within our scene from accessing resource or information or expanding their social network.

Social movements survive repression by creating robust networks. Robust means that any cuts to the network don't cause it to collapse and that there is redundancy of connections for accessing resources or providing solidarity. While some caution is unquestionably necessary, we risk harming our networks and ourselves when we principally base our security on our fears. Our caution should scale with the extent which our activities are—or in the near future will be—criminalized. This means developing an accurate understanding of the repression we face and ensuring our security cultures specifically target those State actions.

Proposal #3: Have Intentional Discussions of Security Culture

Within our groups, our security culture discussions are frequently limited to debating if a single application of a rule is justified or not. We avoid some of the finer points of security culture such as refining practices or changing behavior. People have strong opinions about security and trying to change practices often causes people dig their heels in and resist anything that might be called a loosening of security. They insist on perpetuating practices that create a feeling of safety, and those who want to change a practice often are less invested in changing the behavior than those who want to keep it. Forcing the issue—if we ever actually do it—can create divides in groups, and so in the name of coherence and unity, we avoid them.

The proposal is that we *should* force the issue. Avoiding these discussions and letting pathological security culture practices proliferate harms the movement. If you informally organize, discuss this with your comrades the next time you hang out. If you have formal meetings, make it an agenda item. If

On Power

Anarchism is often defined in its literal sense as being without or against hierarchy. To me, the root of anarchism is to increase individual autonomy, and opposing hierarchy is a natural consequence. If we want autonomy, that which stands in our way is *power*, or more specifically *power over*. Capitalist systems have power over you because they force you to work bullshit jobs to survive. Your landlord has power over you because the need to pay arbitrary rent restricts what choices you might otherwise make. A queerphobic society has power over you because forcing oneself into the closet in order to participate in that society is a reduction of autonomy.

Free choice depends on alternatives existing, and that itself depends on having both knowledge and access to resources. A farmer's autonomy is increased by having greater knowledge of soil, weather, agricultural techniques, or even nutrition which might impact what they choose to cultivate. A disabled person's autonomy is increased by having access to adaptive technologies, alternatives, and substitutes.

Being able to restrict knowledge and resources *is* power, and when phrased that way, it becomes immediately obvious that security culture is—in some ways—at odds with autonomy. Controlling the flow of information to hinder intelligence gathering *inherently* is wielding power over one's current and would-be comrades. Controlling the access to resources—physical spaces, equipment, use of a platform—is again wielding power. These both restrict others' autonomy, even if security culture increases everyone's autonomy in other ways, such as by enabling action or preventing imprisonment. Knowledge gives us more choices and therefore more autonomy.

This isn't to say that we need to abandon the practices of security culture to adhere to some strict definition of increasing individual autonomy. It's just drawing attention to the fact

that there is a tension between the prefigurative creation of autonomy and the need to protect ourselves from threats to our ability to organize. Security culture in part involves holding power over other people, and we need to acknowledge this and do what we can to minimize its negative effects and the extent to which we use it, or at the very least every case needs justification.

The Pathologies

What follows is a description of some of the broad ways that security culture is pathologically applied.

Pathology #1: Reinforcing In-Group Preferences

The first pathological application of security culture is when it is used to create, strengthen, and justify in-group preferences.

There's a conflation that happens between "safety" and "security" not just in intent but in how these words are used. There is only a clear difference in English between these two words. In German they are both the word *Sicherheit*. As they're used in these contexts, secure means being in a state of *actual* protection, at least relevant to the original dangers. Safe means being free of things that cause a feeling of being hurt or harmed (perceived or otherwise), though sometimes it's used to mean free of psychological or emotional discomfort. This conflation of terms leads to accusations of genuine insecurity because of a perceived sense of unsafety.

People who are new aren't trusted because they're unfamiliar. Sometimes they're a little different and don't pass the "vibe check." Maybe this is because they're socially awkward, neurodivergent, come from a different cultural background, or are just having a bad day. New people who don't share to our subcultural traits or adhere to our subcultural norms are viewed

Proposal #1: Embrace Discomfort

There is no singular anarchism, nor is there some utopia where we will never experience distress or discomfort. We will always be exposed to others with differing ideas, norms, and cultural practices. It will never be possible to create in in-group free of discomfort, and this includes of people who might be allies but haven't yet learned—and kept up with!—the rapidly changing vocabulary that aims to reduce harms. There might be places where this method is necessary for the work at hand such as in trauma support groups, but it shouldn't be the default method of all organizing.

We should avoid labeling someone as unsafe or dangerous just because we have perfectly healthy disagreements with them or that they mistakes while learning. Walling people off for perceived or even anticipated differences can be called security, but often it's just simply exclusion in the name of homogeneity. Some people contrast the approach of creating braver spaces (those that acknowledge that conflicts will exist and promise to work through them) with that of creating safer spaces (those that aim to minimize discomfort). The end goal might be quite similar, but the change in framing can drastically shift the norms and group dynamics.

Proposal #2: Critically Evaluate Risk

Not all anarchist organizing is under equal threat. This is abundantly clear, and it's not to say that we should abandon security or be careless for everything but the most risky activities. When we over-apply security culture to casual organizing, we inhibit new connections. This can be by making a scene inaccessible to newcomers by overemphasizing security culture rituals or even not spreading basic information out of paranoia about where it might end up. This prevents people

can be the ones who then place themselves in a leadership position. This too is generalized to not just genuine security but perceived safety. There is a well-documented phenomenon of the individuals with the most conservative stances on a topic driving discourse, and one might see this in debates like whether it's a consent violation to see kink at pride. The demanding security enthusiast might use blocks on consensus to ensure that their needs are met and that the group adheres to their standards. Instead of being a collaborative effort among all to increase collective security, the group's action revolves around the self-appointed expert. Even with the best intentions or when they are actually correct, the person insisting on the most security can dominate a group simply by forcing unattainable security standards on others.

Similar domination via expert knowledge could happen with other forms of anti-repression measures like counter-surveillance or legal assistance, but I have not yet seen this, and it seems rather particular to how techies and security enthusiasts interact with security culture.[9]

The Proposals

The easiest way to attempt to apply security culture is to base it around control of access to resources. A blanket "no" is a simple answer, and once a small group is established, sticking to an insular dynamic is the path of least resistance. It gives a great feeling of safety and even importance by assuming that one's strict security practices makes them relevant. But maybe there are ways to break the cycle and find a collaborative way forward to create a more inclusive security culture.

[9] That said, physical security has the pathology of devolving into cop shit and micro-warlordism, but I (somewhat arbitrarily) draw a distinction between security culture and physical security even though they are quite related.

more skeptically, like if their clothes aren't punk enough or if their interests or hobbies aren't ones we share. Sometimes security culture itself is used as a shibboleth,[3] and if someone thinks to ask the wrong question out of genuine curiosity, they lose social standing or might even be outright shamed for it. Security culture gets used less as a tool for increasing actual security and more as a signal of already belonging.

People use frequency and familiarity as a basis for building trust, and yes, the conversations we need to have to discover shared politics matter, but often it's sufficient that a person has been around at "enough" events to establish some form of "credibility." Varying life paths or even disability can make regularity a challenge, and this method of establishing trust over something like explicit background checks favors those who are likely to be part of the stereotypical anarchist subculture over people might be politically anarchist but lead a different lifestyle. Generally, this creates a boundary between those who are already connected to "the scene" and those who aren't. Those with connections have easier access to spaces, resources, and support. Those without… simply don't.

Voluntary association is fundamental to anarchism. If someone genuinely doesn't want to associate with someone else, that's fine, and they are allowed to create that separation, but also we know we live in a fucked up world of sexism, racism, and the like, so we still need to constantly check our preferences to see if we're expressing some bias that's so deeply internalized that we don't even see it any more. Even further, we don't tolerate the creation of racially segregated enclaves, which is to say: some forms of inclusion/exclusion are considered harmful enough to be fought. We need to be wary of who gets what few privileges our movement affords. Far too often we only make connection with people who are already "like

[3] A shibboleth is any custom or tradition, usually a choice of phrasing or even a single word, that distinguishes one group of people from another.

us," and we use a pre-existing knowledge of security culture as one of the filters. Those who aren't are denied access to helpful information or resources.

Pathology #2: Abuse Enabling

Similar to the strengthening of in-group preferences, security culture can be used to enable abusers. This often happen when someone in a group is called out for problematic behavior, especially more serious accusations of abuse or sexualized violence. The accuser might themself be accused of being an infiltrator or wrecker who is fabricating the accusations purely as a means of disrupting the group. Security culture gets perverted from an analysis of conditions and actions into pure reaction against anything that disrupts the stability of the group. It flips the relation from noting that infiltrators disrupt into asserting that anything that disrupts *must* be an infiltrator. The stability and longevity of the group—and often the most "prestigious" members—are protected over the accuser. This is generally in alignment with who is currently privileged and favors, for example, white cis men.

The accused and their defenders claim that the accusation is harm because it's false, and it's easy for them to point to the "certainty" of the harm the accused claims to be experiencing. The group had the appearance of stability before the accuser brought the abuse to attention. The accused *feels* attacked, and the group must change its focus from their primary tasks to dealing with the accusation, thus there is "disruption." This is pointed out be "obviously harmful and disruptive," and the accuser's claims must be more rigorously proved. The disruption is named as really being the fault of the accuser, and why would they do that if they themselves were the one who is unsafe? So they are cast out and slandered.[4] Or, to quote Sara Ahmed as

[4] For a longer discussion on all this, see the zine *Betrayal: A Critical Analysis of Rape Culture in Anarchist Subcultures.*

Pathology #5: Esoteric Knowledge as Power

Repression is shrouded in a lack of information, and those who can "see" what the State (or other agents) are doing hold some esoteric knowledge that the rest of us do not. Sometimes this isn't easily directly shared as it may only come with significant experience or expert knowledge, though some do try to spread this knowledge as best as possible. One of the most "invisible" kinds of repression is of the information technology variety. We can't "see" our messages being sent around the internet, nor can we "know" they're encrypted. We also can't "see" when we've been hacked or what data the State is gathering on us in the same way we can see jackboots walking on the streets or breaking down doors during raids. In part because of its esoteric nature, and in part because of the strict rules by which information systems operate, there tend to be more cut and dry edicts about digital security relative so the social aspects of security culture.[8]

In many cases, some sort of elite of techies can rise within anarchist circles. They make demands about security, and they shame those who won't or can't follow their rules. Because of the alleged absoluteness of IT security, and because these specialists hold knowledge of these systems, they often use this to elevate themselves over others. Often implicitly, but sometimes explicitly, the claim is that only those who really know security should be leaders, organizers, or principal decision makes. Instead of security being a collaborative effort between equals with different expertises and experiences, the techie asserts authority over others.

This isn't limited to techies in general, but can also come from any people who push security at all. There is some mysticism and ritual in security, and those who have memorized it the best and make the biggest cries for its implementation

[8] Whether or not such strict rules are necessary or effective is another matter entirely.

This centers the gatekeeper in all interactions and ensures that they will be brought into future organizing circles because they have made themselves irreplaceable. This can factor in to decisions on whether to eject them from a collective or not. By avoiding making themselves redundant, they elevate their importance, and they claim they can't be made redundant because doing so would entail sharing private information which violates the established security culture.

In some cases, but not all, this desire to be irreplaceable isn't driven by a lust for power but rather a fear of being replaced. Anxiety is ever-present in our scenes, and financial precarity and harsh social censure for minor transgressions increase fear of rejection and abandonment.[7] Some people position themselves in critical roles to create a sense of safety that the group can't cast them out.

A second way resources are gatekept is a side effect of making a scene opaque and illegible to the State. Information is not made publicly available for events, and activities that are not highly repressed have their details closely guarded. What makes a scene illegible also makes it inaccessible for those that we'd want to join us.

This form of gatekeeping ties in closely with in-group preferences, but it functions slightly differently. Explicit in-group preferences encourage making judgements when a person arrives and then using that to deny them access. This illegibility and opacity is an implicit in-group preference because it is a strong deterrent for those not already connected enough to a scene to have that information directly shared with them.

[7] Widespread anxiety especially in organizing is discussed in the zine *We Are All Very Anxious: Six Theses on Anxiety and Why It is Effectively Preventing Militancy, and One Possible Strategy for Overcoming It* by The Institute for Precarious Consciousness and CrimethInc.

she said in *The Complainer as Carceral Feminist*: "To locate a problem is to become the location of a problem."

The enabling of abuse goes beyond the explicit protection of the abuser themselves. It's often inadvertently reproduced by the broader milieu. As anarchists, we don't only refuse to cooperate with police; we're also mindful that our actions don't aid them. This creates an internal pressure against publicizing an abuser's action. It might delay a callout or restrict what is said within it to make identifying the individual more difficult. We don't want police to learn about rifts in our movement, and if we don't want to provide evidence that might doxx a "comrade" to police or fascists, so we say less. Whisper networks and semi-privately held black books rather than public posts or wheatpastes try to circumvent this issue, but those tactics privilege people already in the know. People new to the scene are far less protected by these methods. Even just making a vague callout or using whisper networks can be labeled a security culture violation because it's exposing "private" internal information to those who weren't "permitted" to see it. At the most extreme end, anti-abuse activists might voluntarily withhold critical information about a violent abuser from people they're trying to warn because it would be "doxxing" to do so.

In these cases, even well-meaning comrades can prioritize the safety of the abuser over other comrades or potential future targets. What's overlooked is that the risk of the abuser harming again is far greater than the risk of a State response to that information being made public, and moreover that someone who has intentionally caused harms has forfeit their right to unlimited protection. *They* are the danger we need protection from.

Pathology #3: Clout Seeking

While it is an ideal held—especially by anarcha-feminists—that all forms of work within the anarchist movement should

be valued, there is undoubtedly a hierarchy where those who engage in violent direct action are held in greater esteem than those who don't. This comes in part from the fact that we see those who are more willing to take risks as being more "dedicated" to "the cause" or as being better allies or accomplices. It's true to some extent as the converse is true: those who are unwilling to expose themselves to any risk tend to be unreliable comrades.[5] The result of this ends up where we give social capital to people who engage in direct action or otherwise take risks, regardless of whether or not they're sensible. However, we end up with some series of logical jumps where we assume the causality between dedication, risk-taking, and the need for security is far more pronounced than it actually is.

A large part of security culture is The Two Nevers:[6]

> 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 means we don't—or at least shouldn't—actually know who is allegedly doing all this super cool shit, and people know they shouldn't be so obvious about naming themselves as the doers of cool deeds, so we look for people who hint that they are. We look for people who make a scene of their security culture through indirect bragging.

Indirect bragging is when someone doesn't directly say that they engage in criminalized activity, but they do everything that can to ensure that people assume they do. Following a big action, people might say that they attended since this is expected of most radicals in a scene, but the indirect-braggarts

[5] Risk is relative to one's personal situation and local context. Posting about being an antifascist could be more risky for some than directly confronting fascists is for others.

[6] This term and the nevers themselves are pulled directly from the zine *Confidence Courage Connection Trust: A proposal for security culture.*

will make a show of stating that they can't talk about whether or not they were at an action (instead of simply saying "nah, stayed home"). More generally, they might make a big deal of telling you how they can never talk about what sort of organizing they're doing or where they were on any given weekend. People "ooh" and "ahh" at their showmanship and then give them the clout they're do desperately seeking. Because we don't actually know who is carrying out these actions, we end up applauding people who suggest that they are the ones who did.

This behavior feeds off of and reinforces the supremacy violent direct action holds within anarchist milieus. It creates a hierarchy whereby those who—irrelevant of whether or not they even do any direct actions—can elevate themselves above others. A social elite can develop by draping oneself in aggressive security culture.

Pathology #4: Gatekeeping Resources

Under severe repression, the use of cell structures becomes necessary because of draconian response against anarchists and other activists. This cell structure is rarely necessary, and yet we apply it to day-to-day organizing under broadly permissive "liberal democracies."

Part of security culture is that everyone gets to choose their level of risk and that everyone is allowed to consent to what risks they take and what information is shared about them. This includes sharing a phone number or email address. Naturally, if someone asks for another's contact details, we shouldn't give it up without explicit consent. This norm is good and healthy.

What can often happen is that one person will act as a gatekeeper between multiple collectives or even social circles. This allows that one person to mediate all interactions and even directly preemptively gatekeep access between the collectives.