What the Corona Virus Pandemic Can Teach Us About Security Culture

By Håkan Geijer
With Illustrations by zer0coil

Security culture is fundamentally about collective action to identify and mitigate risks. Police can read SMS messages, so your crew uses an encrypted chat app. Local fascists might learn your identity and show up at your home or place of employment, so you use a fake name and pseudonymous online accounts. Counter-protesters at a nazi march might get arrested, but the risk of rising fascism is greater, so you accept the risk of arrest and put your body on the line.

We've picked up many of these OpSec[1] tips in a piecemeal fashion as we joined activist circles. Maybe your first experience with security was being asked to leave your mobile phone in a box outside the room where a meeting was taking place. Or maybe it was being told to hide your face from right-wing press at a demonstration. Many people feel that their involvement in liberatory movements does not necessitate much security, so they've never developed holistic security practices. Of the many who do recognize the need for security, these practices have become so habitual that they happen without conscious thought.

It is rare that there are paradigm shifts in our security practices either because of changing circumstances or new technologies. These things often happen slowly and in ways we don't notice until we retrospect over long periods of time. We don't have the opportunity to see a drastic change and compare how things were before and after.

In our daily lives we have at least an inkling of a concern about our protecting our health from disease. We wash our hands after we go to the loo or take our shoes off in the entryway of our flats. Many such practices can be cultural, and they are often habits we picked up one at a time but hardly think about.

The COVID-19 pandemic has been a shock to many people who previously were rather lax about protecting themselves from diseases like the flu or common cold. In a short period of time, the majority of us went from having no real threat model of how we might get sick or what the consequences were, to being acutely aware of a threat that was all around us. Most were unaware of how many died yearly from the cold, if they even knew it was killing people at all. The new threat to our health from the corona virus forced us to make massive changes to our perception of the world and our behavior as we navigated it.

Security is often taught via analogy. Encryption is explained by describing two parties sending letters to each other via some special kind of post. When we talk about the security of the individuals in a group who live in disparate locations, we use metaphors about the physical security of a building. The aphorism "all models are wrong, some are useful" comes from the statistician George Box who nearly a decade before more eloquently said:

[1] Operational security.

> For such a model there is no need to ask the question "Is the model true?". If "truth" is to be the "whole truth" the answer must be "No". The only question of interest is "Is the model illuminating and useful?"

Using the pandemic as an analogy, this text explores how protecting oneself and others from disease is remarkably similar to developing a security culture to protect against repression. The descriptions of the pandemic focus on how it was experienced in Europe. Some of the experiences that will be described are rather generalizable. Others may be less so as they are the experiences of my particular radical circles.

There are many definitions for security culture and OpSec, so to provide clarity I'm using the two definitions here as this is generally how they are used by activists.

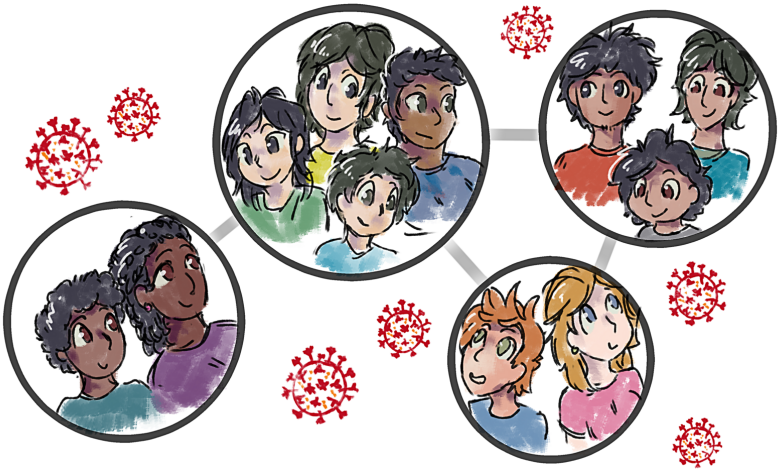
> **Security culture** is the set of norms with a social group or movement designed to counter surveillance and disruption either from the State or private entities such as militias, far-right gangs, or corporations.
>
> **Operational security** is the set of specific practices an individual can take that reduce surveillance and disruption.

Leaving your phone at home for an action is OpSec. Your affinity group normalizing the practice that everyone leaves their phone at home is security culture.

Pandemic Pods and Affinity Groups

Early in the pandemic, we were encouraged to form pandemic pods, or rather closed social groups. The idea behind these closed groups rather than the naturally forming webs of human connection was to limit the spread of the disease. If one person in a pod got infected, the whole pod might get infected too, but it would be limited to just the few people within that pod. While this practice complicated by living situations (those with roommates) and working situations (those who couldn't work form home), it still provided one way of limiting the spread.

Goals of security culture are to reduce information leaks, prosecutions, and violence faced by its practitioners. Affinity groups (AGs) are closed



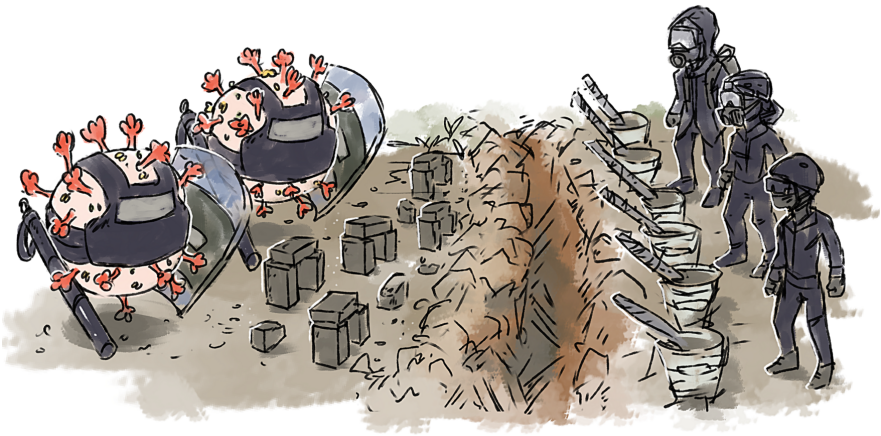
groups of trusted individuals that form in part to carry out political actions together.[2] The closed nature is in part due to the threat of informants or infiltrators. AGs can plan political actions without worrying that their plans will be overheard, and if they agree to silence, they can carry out these actions knowing that no one but the members of the AG will know who did it.

Affinity groups are robust against infiltration and State-led disruption in much the way pandemic pods—when employed correctly—are robust against viral transmission. Loosely networked AGs exist in opposition to classic organization structures like political parties or NGOs. Leadership in classical structures often has an overview of all members including what they are doing, and members may shuffle between working groups or task forces within these structures. Infiltrators and informants can rise in the ranks to see everything or float through the working groups collecting information on everyone because they are granted implicit trust by merely being a member of the organization. Vanguardist political groups and so-called "big tent" organizations are the equivalent of superspreader events in terms of infiltration and information leakage. If the "disease" is having your details gathered by the police, "infection" spreads rapidly in these groups. Organizing via AGs helps prevent infiltration and information leaks.

[2]Sometimes these are called cells, but that term is used somewhat derogatorily and has connotations of terrorism or militancy. Affinity groups can form for many reasons.

Defense in Depth

Health measures that have been emphasized over the pandemic include avoiding in-person social contact, maintaining distance when around others, ventilating indoor spaces, wearing masks, frequent hand-washing, and the sanitization of surfaces. There was not just one panacea, but many steps we were told to take. Each of these on their own contributes to decreased viral transmission, though some more than others. If an individual enters a shared space with only a surgical mask, they may still be significantly protected by everyone else wearing FFP2 masks. If everyone wears only surgical masks, they are once again protected by ventilation and air filters in the building.



Defense in depth means using more than just one control against a single threat. Sometimes these controls are additive such as when two individuals wear masks, the first has a lower chance of being infected by the second than if only the first or second alone wore a mask. Sometimes these controls are simply redundant such as disinfecting surfaces, frequent hand-washing, and avoiding touching one's face while out in public. These controls protect against the same vector, namely infection via transmitting the virus to mucous membranes after touching surfaces that are infectious. If someone doesn't wash their hands, keeping surfaces clean still protects them. If someone breaks the habit of frequently touching their face, the risk of infection from going long periods of time without hand-washing is also reduced.

Likewise, good OpSec and security culture use defense in depth to prevent information leaks or disruption. To implement this, one can ask themself: if this control fails, is there another that prevents my adversary from achiev-

ing their goals either partially or completely? Because your phone might be seized and searched, you might have device encryption and a strong passphrase, but moreover you might enable disappearing messages to reduce the amount of recoverable material on your device if it is compromised. Maybe all these layers of defense will eventually fail, but often it's better if they fail after 1 year than 1 day. If your AG agrees to a code of silence about secrets, you can further prevent accidental information leaks by not telling them about your past hijinks. One layer of protection is their silence; the second layer is yours. When making a plan for your and your AGs' security, plan for many layers of defense.

Overreacting

Another part of the early pandemic was the attempts to counter the skepticism people showed toward the effectiveness of countermeasures like masking and avoiding in-person contact. There were trends on social media and statements from public health officials saying things like "if you feel like you're overreacting, you're doing it right." Others said things like "if there ends up being no pandemic, you might feel like you made sacrifices for no reason, but that's proof it worked." Many people pointed at the Y2K bug[3] as an example where disaster was averted due to what felt like an overreaction.

Messaging that tried to normalize the idea of overreacting was not just

[3]A problem where computers used two digits to represent the year so that `00` made `1900` and `2000` indistinguishable. There was minimal damage from this bug because of the large amount of effort experts put in to correcting it.

about motivating people to put in the effort themselves, but also to help them overcome the feeling of foolishness for taking action others might not. Maybe you felt ridiculous for wearing a mask before anyone else at your local market was, and maybe your friends told you that you were being paranoid by avoiding cafes and restaurants when there were only a handful of reported cases. Maybe you told off your friends for stocking up on non-perishable goods in case they got quarantined or there were neighborhood lockdowns like in Bergamo.[4] Avoiding action is often done to avoid being shamed by others, and these criticisms are often justifications to oneself. Telling someone off for taking action makes you feel better about not taking action you suspect you should.

With activism, you don't notice the arrests you prevented or the doxxes that didn't happen because of good security culture. Maintaining a sustained high-level of security can feel overly paranoid or like wearing a tin-foil hat, and of course there are many genuine cases of overreaction ("No one should ever use mobile phones!"), but often in radical circles, security practices are dismissed as going too far. A virus can only infect you at the time of your exposure to it, but data lives forever. An email you sent or security footage can come back to haunt you years later, and governments can retroactively criminalize previously legal activity as part of a campaign of repression. The pandemic aside, masking all the time may be unnecessary, but practicing security culture is always prudent.

Misinformation

When we think of misinformation in the context of the COVID-19 pandemic, we often first think of the strong misinformation machine that gave rise to people eating horse dewormer or claiming that the various vaccines were part of an NWO plot to put microchips in our brains. Many other beliefs based on various "alternative facts" also waxed as the pandemic went along like naturopaths pushing urine therapy. More subtle were the lies that were pushed early on like the claim that novel corona virus was just "the common cold." Late in the pandemic, even more liberal sources and radicals themselves were claiming that the omicron variant "wasn't that bad." Misinformation based on uncertainty is no stranger either. Early in the pandemic, people decried masking as they weren't sure it was effective despite corroborating evidence from other regions for other disease outbreaks. When the vaccines rolled out, there were claims that they were rushed through safety checks and that they weren't safe because we didn't yet know the long-term effects, something

[4] An city in the Lombardy region of Italy. It was the first wildfire corona outbreak in Europe back in February of 2020.

most prominently seen in the panic following a miniscule number of cases of blood clots. It was true we didn't know the long-term effect because of the linear nature of time, but extrapolating from the billions of other vaccinated humans for dozens of diseases, it was safe to say that the long-term effects were negligible to non-existent.

While we were able to point at many of these things coming from the establishment, there was significant misinformation that came from radical spaces. Like many conspiracy theories, they stood to benefit the person spreading them and weren't accidental misinformation. Tankies made claims of China's flawless response forgetting the initial reaction was to arrest the doctors who reported on what appeared to be a SARS[5] outbreak. Pundits and influencers spread anti-vaxx conspiracies because being vaguely contrarian is part of their brand, and stirring controversy gains them attention and the associated clout and donations. Some BLM-adjacent[6] cult-like groups and egotistical influencers said that "white medicine" or "imperialist vaccines" couldn't be trusted and that the vaccine was just Tuskegee 2.0, thus implying that said groups or individuals were the only ones uniquely able to spot these abuses and therefore protect their members or followers.

These corona virus and vaxx conspiracies are difficult to debunk because they contain grains of truth. The NHS, WHO, CDC, and similar have made contradictory statements, so there is reason to doubt what they say. The Tuskegee Syphilis experiment was real, and medical racism has not gone away.

[5]Severe Acute Respiratory Syndrome.

[6]If BLM is the loose coalition of anti-racist activists, then like all movements there will be wingnuts. I mean this as no denigration of the movement at large because of course all black lives matter.

Healthcare is run for profit, and there are dangerous medical products that haven't received enough scrutiny. Starting from a position of skepticism or even uncertainty is valid, but failing to analyze further from this position is harmful.

If we ignore the atrocious security practices of conservative and fascist groups, we can still see that security is a discipline within activist milieus where misinformation runs rampant. Some poor security practices are furthered because of what individuals or orgs are trying to peddle. Livestreamers are defended as being necessary for the cause ("Good propaganda!") despite only dubious claims of the benefit of riot-porn and the obvious harm to those arrested because of the evidence the streamers generate. Large organizations downplay State infiltration efforts because they rely on the strongman illusion of infallibility or the belief that absolute numbers is the primary goal of movement building. People who call themselves organizers will elevate themselves as doing radical praxis the "right" way by chiding and shaming those who hide their names and faces, and they take this stance because their "importance" to the movement is dependent solely on them being a loud voice with a name and a face. Some of the misinformation is—like medical misinformation—many people simultaneously reaching the same wrong conclusions without malice as we often see in the smart phone vs. dumb phone debate.

Like how we looked to virologists and epidemiologists to inform our response to the pandemic, we need to look to security experts to inform our security culture. Experts may be individuals who work in cybersecurity to teach us about encrypted chat apps, but just as well this can be seasoned members of the movement who have lived through occupations, police raids, and repressive legal cases. We need to agree on the basic facts of the world if we are to analyze it. Misunderstanding the internet and encryption will lead to poor IT security. Inaccurate models of how the police and legal system enact State repression will lead to inadequate countermeasures. To avoid repression, one needs an accurate threat model, and an accurate threat model necessarily requires an accurate model of the world. Do not let yourself become clouded by dogmatic adherence to your ideology or the words of your heroes. Beware people who claim "I do this, therefore it is correct." Seek facts and strongly supported theories.

At-Risk Groups

The corona virus did not affect us all equally. Some individuals were at greater risk because of factors like their age or medical history. Others were placed at increased risk due to their working conditions. Those who could work from home had particularly low rates of infection compared to those

forced to work service jobs. Affluence afforded additional layers of protection like better access to preventative measures, testing, and treatment.

The threat individuals and orgs face from the State or other malicious parties is not equally distributed. Some of us have traits we are born with that massively change how we are surveilled and treated by the State such as our skin color or what passports we hold. Others develop traits over time—like blossoming queerness or a radical political position—that attract scrutiny from the State or conservatives at large. Like with preventing infection, money plays a roll in preventing repression. More expensive electronics often provide better security, and being able to throw clothes in the bin after a risky action is a luxury.

The early pandemic placed a strong emphasis on doing one's part to protect at-risk groups. It leaned in to the sense of altruism many of us have to help a neighbor. We all masked up and stay home to save our nans and the immunocompromised. It worked, and almost *too* well as many people who weren't in at-risk groups believed they had *no* risk.

Security functions in much the same way. If only the most active radicals hid their activity, they would stand out from the crowd. Good security also functions by obfuscation. Poor insight into groups means surveillance needs to be deployed against more targets and infiltrators need to target more groups. You may feel that you're not personally at-risk, and you may think—wrongly—that no one in your circles is at-risk, but adopting stronger security practices helps provide cover for those who most critically need to avoid disruption, and furthermore it helps protect *you*.

Crisis Fatigue

Many people who took the pandemic seriously from the onset found themselves unable to maintain their precautions as time went on. The routine of hand-washing upon returning home may have become hand-washing "only if I think I touched something gross." Consciously avoiding indoor gatherings may have slipped into justifying going out to a friend's no-mask birthday party. This phenomenon has been called "pandemic fatigue." Sometimes people stop following preventative measures because they simply don't want to or find them fucking annoying. Other times it's the belief that they earned a cheat day by being so good for so long. Some people see the pandemic as never-ending and can no longer rationalize giving up so much for so little perceived benefit.

I'm not claiming that our FOMO[7] is baseless. We've all given up on attending weddings or funerals, hosting birthday parties, or traveling to see friends and family. How many regular social activities like hanging out at home, going to a favorite pub, or spontaneously catching a movie have we missed in the last two years? It's not even just the voluntary measures we've taken, but seeing that others aren't taking them, so why should we suffer while they go out and party? Maybe it's even seeing the intentionally poor response of the ruling class that makes so many of our individual efforts seem worthless.

But just because we're tired and burned out doesn't mean the pandemic is over. This winter has been particularly harsh for many of us: a second winter into the pandemic after the summer that wasn't, all with the backdrop of pandemic-related scandals, soaring infections, and sustained fatalities.

OpSec fatigue is just as real. Nearly every security measure we take has some cost. Abandoning WhatsApp after they changed their privacy policy meant losing out on communication with those who hadn't switched to Signal. Leaving phones at home for actions complicates coordination. Using multiple devices for multiple aliases means more shit to constantly lug around with you. Refusing to organize direct actions with people who have poor security practices leads to conflict in meetings or solitudinous actions.

Because of these costs—either material or "merely" mental—people often relax their security standards, but the threat of surveillance and disruption do not disappear because we lose interest. The longer one is in radical movements, the more they tend feel the pressure of external threats. This stress can make it hard to maintain the desired level of security. There's also the mistaken belief that actions taken during periods of relaxed security not leading to arrest is proof that the reduce security is still secure enough.

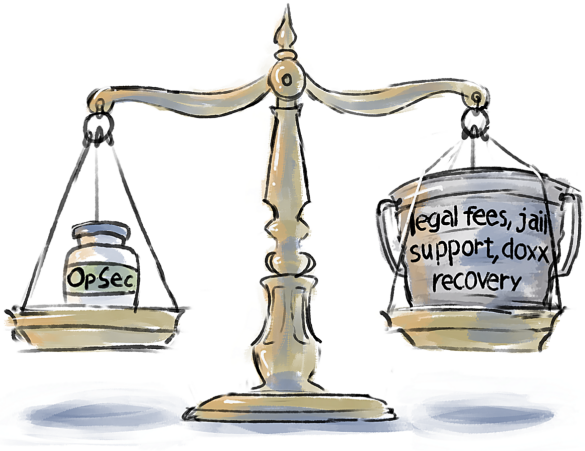
[7] Fear of Missing Out.

With the corona virus, many people have been burned out and resigned saying "we're all gonna get it" before giving up many of their precautions. Many activists develop a view known as security nihilism which amounts to believing that no amount of security can prevent repression, so why bother with any of its encumbrance?

Crisis fatigue is a hard problem both for the pandemic and for security, and I cannot pretend to have a clean solution. My own experiences and those of others suggest that at least OpSec fatigue is countered by a stronger security culture. If all your friends wear masks and only make plans outside, it's easy to go along with them. Likewise, if we have each others' backs with our security, the small slips we make are more easily corrected. It's also easier to be secure when everyone around you is too instead of constantly fighting to just barely attain a low baseline of security.

Prevention, Not Cures

Even where there is widespread deployment of the corona virus vaccine including 3rd booster shots, there are no specific and effective treatments for COVID-19. Care is supportive. Individuals can keep themselves fed, hydrated, and rested to help improve their ability to fight the disease and recover. Even when receiving intensive care, much of the treatments patients receive is not to eradicate the virus but to fight its effects on the body. Recovery from "mild" COVID-19 can take weeks, and the individual may develop temporary or permanent disabilities as a result. Moderate and severe cases require costly treatment at specialized facilities with limited capacity.



On the other hand, prevention is simple, cheap, and does not require specialists to be effective. Even the cheapest surgical masks have a marked effect on reducing viral transmission, and skipping the pub to take a walk through the city is free.

There is always some cost to prevention. Masks, even reusable cloth ones that are washed daily, cost money. Bulk hand sanitizer also has some cost. Much of the cost is psychological. Avoiding gatherings takes a mental toll, and isolation can lead to depression. One can get fatigued by always asking "is this safe?" or foregoing desired activities. Even if the chances of getting the disease is low, people may weigh these preventative measures as being too costly and accept what they see as tiny a risk of life-altering outcomes.

Security is also a case where an ounce of prevention is worth a pound of cure. The bother of getting all your contacts to switch to an end-to-end encrypted chat app might have some upfront and upkeep costs, but this effort is drastically lower than the response necessary after being prosecuted. Dressing in Black Bloc at actions and having clothing to change in to when traveling to and from the action can be bothersome—especially in summer's heat—but this is a small price to pay compared to the damages of being arrested or doxxed with possible subsequent stalking and harassment. Every arrest that is prevented means more time legal aid can spend on other cases. Every comrade who doesn't have to move flats because of fascist harassment is funds that can be redirect to the community. Every imprisonment that is avoided means a healthier community that isn't mourning the abduction of a comrade and exerting effort for appeals or prison support.

Like we saw early in the pandemic, one of the goals was to "flatten the

curve." If it was assumed that some fixed cumulative number of people would require hospitalization, it would be better for that number to be stretched out over 1 year rather than 1 month. If there was even some Universal Truth that all activists had some fixed chance of imprisonment, it would be best to spread this over a longer time thus giving them more time to act before being taken off the board and more time to gather resources to support them. This certainly isn't the case, but the goal should be to prevent and delay consequences of repression as long as possible.

Even when looking at the State level, many of the justifications for avoiding the upfront costs were to avoid economic downturn from lockdowns and missed work. The result of poor containment was that these consequences happened anyway. A lack of security culture may have a short term benefit of alleged increased effectiveness ("Better recruitment and more reach!"), but the downside can be disruptors ravaging a scene in ways that require great expenditures to rebuild. The benefit of a strong security culture outweighs the near-term costs of developing it in the first place.

Security Theater, Expectations, and Nonadherence

Some initial measures taken to slow the spread of the virus were ineffective because they were based on poor or missing information. Individuals who cared about managing the spread of the virus wanted quick solutions, and often this was in the form of superficial measures that gave feeling of effort rather than tangible results. Policy makers wanted to show strength and that were were doing *something*, so they did *anything at all*. Ineffective countermeasures that give merely a feeling of security or action taken are called security theater. In the case of the pandemic, we saw this with use of chin-strap sneeze guards rather than masks, or the use of disposable nitrile gloves when out in public yet the wearer still constantly touched their face. Other larger instances of security theater were spraying disinfectants into the air from vehicles or requiring masks while walking through sparsely populated public parks.

Security theater in its original sense is often present as a significant influence on security culture. Often this is done by either intentional or accidental conflation of "feeling unsafe" and "being in danger." Safe spaces—in the sense that they feel safe regardless of risk—are often needed for healing, and this is not decrying them, but inaccurately naming threats for many spaces is security theater. Queer spaces that don't allow "straight" partners as a means to keep out the abusive cis-hets is security theater (because queer people can be abusers too, obviously). Radical spaces that shun people who

"look like cops" (i.e., middle-aged white men) likely have a very high false positive rate, and the fact that there is enough "diversity" in local and federal police means that infiltrators could be of nearly any demographic. Security theater also happens through misunderstanding such as telling someone to use a VPN to avoid being tracked on the internet[8] or to use a dumb phone to prevent location tracking.

As corona measures became normalized, those who cared about minimizing their risk would look for clear signals of the measures. This might be be presence of signs requiring masks before entering a building, or conversely avoiding establishments that forbid masks. In this sense, declarations of adherence were not just invitations for other risk-avoidant individuals, but were deterrents for risky individuals. However, as time went on, these posted signs and online announcements became less meaningful as they were not always voluntarily enforced. Events might loudly claim to require masks plus proof of vaccination plus a test, but then totally fail to check those or even if one was showing up at their booked times.

Security culture often suffers from a similar lack of enforcement. Posted bans on photography in a radical space are meaningless unless people actually stop others from recording. Actions that are declared as phoneless still occur if some participants bring phones because "fuck it, they're already here." People loudmouthing on social media are not ostracized when they endanger others. It's not enough to declare an ideal. The ideals need to be

[8]VPNs do not in a general sense stop tracking or provide anonymity. In limited cases, such as simply hiding your IP address from a website's operator, they provide some protections.

enforced by some means or another.

The social cost of nonadherence to corona measures can be rather high. It can mean exclusion from a group activity such a requiring everyone to be tested before attending. Many vaxx-"skeptics" or anti-vaxxers admitted to feeling shamed about their position, so they started lying about it. When dating—or more generally, when meeting new people—the threshold for expected adherence tends to be higher. In much the way that partners lie about their condom use or STI testing frequency, telling a new person "yeah, I'm safe with corona" and listing a few key phrases has become a very noisy signal as many people know what they're expected to say even if don't actually do these things. Moreover, what two people consider safe can greatly vary. Making someone name what they do exactly including specific activities is considered invasive and awkward. Clear communication would allow two people to have accurate knowledge of each other's measures which might mean that the person being lax about theirs has to face immediate consequences for them. Lying or deflecting is manipulative and violates consent, and it endangers the other party who is trying to minimize risk.

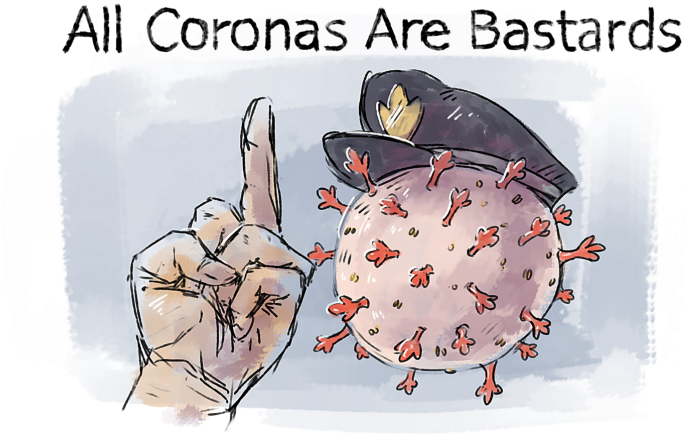
When groups practice security culture, there are too few conversations about the exact nature of the security model they are operating on. There is not a shared language, and simply saying things like "we practice anti-repression" or "we're secure" can be meaningless unless the specifics are discussed. Individuals who have poor security practices or have risks often don't declare them. Addiction is one such case that can lead to sloppy practices or exploitation by the State,[9] and its presence is often hidden for complex social reasons. Other behaviors that have been security risks are relationships (sexual-romantic, platonic, etc.) with people on the right, and while this is unconscionable for many reasons, I'm flagging it as it specifically is a massive security risk to one's comrades that is kept hidden for personal gain.

To avoid the harms—both accidental and manipulative—from poorly communicated security practices, we need to normalize explicit discussions of security models. Abusers and the selfish will always lie, but this at least gives a starting point, and as it's said: trust but verify. As the need for security increases, often as a result of the activities one's group carries out, these discussions need to become more frequent. The level of detail needs to increase, and the claims need to be more strongly verified. Being a loudmouth on social media with a hot temper may be fine from a security perfective for a local Food Not Bombs chapter, but it may be unacceptable for a tightly knit affinity group that carries out direct actions. Groups that carry out

[9] I have no problem with substance users or enjoyers, and I do not think all users or people with addictions are inherently dangerous. It is just that the presence of addiction is a complicating factor that increases the risk of repression.

high-risk activities may want to recede from the scene at large and implement a ban on individuals taking part in other actions because the possibility of an arrest for tagging a building could draw far too much attention to the other more secret actions. Clear and explicit communication, and the trust it is built on, are necessary for effective security. Like with the pandemic, we've had to (temporarily) cut people out of lives for poor adherence, and our affinity groups may have to do the same for those who lie about or fail to practice security culture.

Throughout the pandemic, we have seen that we have shifting models of what constitutes risk, and we have seen the threat landscape rapidly change. First there was the virus, then the vaccines, and next the viral variants (and there will be further changes too). Some people may have had kids start school which created a new vector for infection, and others have had life changes that caused a shift in their individual threat model while others saw no change. These shifts require us to re-model our risk to counter it.



By looking at how we reacted and created safety for ourselves and others—or at the very least reduced risk—we can see patterns in group behavior that mirror group behavior with respect to security culture. Learnings from the pandemic are more concrete despite the somewhat abstract nature of the virus (one can't see it, and maybe one's friends all remained uninfected, but the threat is there). These observations and lessons about modeling and reducing risk can be applied to security culture. Many of the poor responses to the pandemic have analogues to poor responses to repression.

Like how viruses spread through populations, so too spread the harms of repression. The pandemic has rising and falling waves of infection that affect the population unevenly, and we see the same with waves of repression. Zero-risk of infection by the corona virus is near impossible as is zero-risk of disruption by State and non-State actors. Using many tools, such as studies or analogies, one builds a threat model for themself and their crew, and through this model informs a security culture that counters surveillance and disruption. "We keep us safe" applies to our health and our liberty. This mutual regard for one another's well-being is fundamental to security culture and is the base for effective and enduring radical movements.

It is rare that there are paradigm shifts in our security practices either because of changing circumstances or new technologies. These things often happen slowly and in ways we don't notice until we retrospect over long periods of time. However, we can emphasize the changes we've made to our daily lives during the pandemic and use these practices as analogies to explores how protecting oneself and others from disease is remarkably similar to developing a security culture to protect against repression.

2022