A Base to Stand On

Distinguishing OpSec and Security Culture

Sometimes related terms become synonyms, and sometimes that can be fine. English is full of them, like "amazing" and "awesome"—no one misses the difference between these words.

Sometimes though, allowing the difference between terms to get lost also causes us to lose a useful piece of meaning. Operational security (OpSec) and security culture are two terms that have similar but distinct meanings, and both are required parts of an anarchist practice of security against repression.

OpSec refers to the specific practices used to avoid getting caught for a given action or project. Some OpSec practices include wearing gloves and masks, using different shoes, measures to avoid leaving DNA, black bloc clothing, using Tails for anonymous Internet access, and so on. OpSec is on the level of the action or project. These practices can be taught, but ultimately only the people doing a specific project together need to agree on which OpSec practices to use.

According to Confidence Courage Connection Trust:[1] "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." Security culture occurs on the level of the relationship or the network. These practices need to be shared as widely as possible to be effective.

At first glance, OpSec might seem more important. If we have the practices we need to be safe, the thinking goes, then what does it matter what other people in the milieu do? Many anarchists are (justifiably) skeptical of milieus and don't see themselves as connected to or reliant on people they don't have close affinity with. A lot of energy in the anarchist space goes into perfecting OpSec, which seems appropriate, since if you want to take offensive action, it's preferable to not get caught.

However, security culture is also important, and good OpSec is no replacement for it. It provides the social context—the base—on which all our activity is built. Because, like it or not, we are all embedded in networks, and the price of fully cutting yourself off from them is high. Without a stable base, it is much harder to take action safely.

[1] https://notrace.how/resources/#confidence-courage-connection-trust

Going back to Confidence Courage Connection Trust, the authors write that security culture is not about closing up, but finding ways to safely stay open to connections with others. It involves having honest conversations about risk and setting some basic norms with broader networks than just the people we intend to act with. Security culture is not static—it's not just a set of rules that people in "radical" subcultures should know. It needs to be dynamic, based on ongoing conversations and our best analysis of current repression patterns.

Practices like vouching, network mapping, and background checks might seem like OpSec and may be an important part of planning certain actions, but they come out of security culture. Security culture involves asking, "what would it take for me to trust you?". It doesn't mean you need to vouch everyone you know or that you don't spend time with people you don't vouch, just that you're clear about who you trust with what, and why, and that you have mechanisms for learning to trust new people safely.

No amount of good habits about how to talk about actions that occur in your town (security culture) will protect you if you leave DNA at the scene (OpSec), and no amount of detecting physical surveillance (OpSec) will protect you from the undercover cop who befriended your roommate in order to get close to you (security culture). OpSec and security culture practices are distinct and one is not a substitute for the other. By developing a more thorough understanding of both frameworks we can try to keep ourselves and each other out of prison while continuing to build connections and expand informal networks of affinity.

Operational security (OpSec) and security culture are two terms that have similar but distinct meanings, and both are required parts of an anarchist practice of security against repression.

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.