find each other.

Counter-Surveillance Resource Center
CSRC Bulletin #1
2023

Retreived on 2023-03-31 from csrc.link

lib.edist.ro

CSRC Bulletin #1

Counter-Surveillance Resource Center

2023

International Coordination Against Targeted Surveillance

We are anarchists. We believe in an international coordination of informal anarchist groups to pursue the fight against all forms of domination. We believe that sharing knowledge about our enemies' capabilities and tactics should be an important part of that coordination. The knowledge is not an end in itself, but a means to limit our chances of being caught so we can continue attacking.

Our enemies have great capabilities and perfected tactics. On their side they have the police and justice systems, the scientists and technocrats, and in some cases the support of the general population. They control vast infrastructure networks. They have infinite memory, archives and DNA databases.

On our side, we have the informal and decentralized nature of our organizations, shadows to hide in, and solidarity to help each other in difficult times, to continue the fights of comrades who cannot do so anymore.

> No matter what, we make and will continue to make mistakes in the battle against such strong oppressive mechanisms. Mistakes that will always ”cost” more compared to the cops' mistakes which are ”absorbed”. We must weigh the situations again and ensure that the mistakes which happened once simply can not happen again. We must study and appreciate the accumulated experience of so many years and, taking into account the tendency to prepare for the battles which already took place and not for those that will come, let's be prepared and may luck be on our side…
>
> — anarchist comrades from Greece, in a text detailing the surveillance that led to their arrests, 2013

Our enemies already organize on an international level; they share information, tactics, and technological and scientific developments. This is unfortunate, but it also means that a report by comrades in one country — on, say, a good way to deal with DNA traces, or a bug found in a squat, or a cheap tool to take down police drones — could help others anywhere else in the world.

Certainly, not everything should be shared publicly. Sometimes, information still unknown to our enemies should remain secret based on a specific strategy or plan. But otherwise: let's share knowledge and experiences, and organize ourselves!

Announcing: The Threat Library

The goal behind the Counter-Surveillance Resource Center's newly released Threat Library is simple: looking at the state's array of repressive techniques and in order to better outmaneuver them.[1] The Library documents two dozen different policing techniques, splitting them into three tactics (deterrence, incrimination, and arrest), and offering potential mitigations, meaning ways of reducing damage, for each one. It also connects techniques to specific repressive operations carried out by the state against anarchists in the past couple of decades.

The Threat Library is meant to help you threat model, a process through which you try to understand what kinds of measures the state is likely to be taking against you so that you can prepare for them. This exercise is best done collaboratively with the comrades you are working with on a specific project. Good threat modeling can transform fear or paranoia into courage, by giving us a specific idea of what we are up against so we can take precautions. In other words, it helps us decide on appropriate Operational Security (OpSec).

[1] `https://www.csrc.link/threat-library`

The CSRC suggests using the Threat Library to make ’attack trees’. ”Attack trees are a tool to facilitate a collective brainstorming exercise on the different ways that an adversary could successfully attack you in a given context, by representing the attacks in a tree structure.” See the Threat Library tutorial for a step-by-step guide on their use.

The Threat Library can also be used to navigate resources outside of a threat modeling exercise. Suppose that anarchists in my area have a history of infiltrators and informants being used to break up our organizing. Under the ”Incrimination” tab, I select ”infiltrators.” In no more than 300 words, the entry breaks down the five main types of infiltrators and offers three possible mitigations (attack, need to know principle, and network map exercise). If I click on the ”Infiltrators topic” button, I’m given a list of 27 texts written by anarchists about infiltrators in their networks. My fear of infiltrators is eased by knowing what specific signs to look for and with some practical tools for strengthening my networks of trust.

With topics ranging from door knocks to house raids to forensics, the Threat Library aims to be thorough while also staying brief and to the point. The CSRC has a huge amount of information about repression and how to deal with it, and the Threat Library summarizes and sorts it all for you so it’s practical and easy to parse. The Threat Library is available in zine format for easy reading and distribution.

Is there a technique, mitigation, or repressive operation that you think is missing? Would you like to edit one that is currently listed? To add, improve, give criticism or feedback to the Threat Library, get in touch with us at csrc@riseup.net.

9. be unreachable by phone, be social

10. fuck technology

from Rumoer n°5, ”Ten tips to trash telephones” video analysis worries many comrades. With this insight we want to show possibilities to resist against this surveillance technique.

Contribute to CSRC!

We propose to use the CSRC website to facilitate the sharing of knowledge and experiences on the topic of targeted surveillance among comrades.

Browse our 180+ resources at csrc.link, which is also accessible in Tor Browser through an .onion address.

Print our brand new stickers and spread them around.

Contribute by sending us an email at csrc@riseup.net - if you want to encrypt, our PGP key is here.

Ten Tips to Trash Telephones

1. set your phone on fire
2. throw your phone in the canal
3. put your friends' phones in a bigger fire
4. throw all phones in the canal
5. don't always bring your phones (someone might throw it in the fire)
6. talk to each other, not to your screen
7. destroy evidence (back to tip 1 and 2) and don't let others make evidence (back to tip 3 and 4)
8. make phone use a topic

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: "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.

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.

Snippets Against Surveillance

In this section, we'd like to share short notes that are within the scope of the CSRC, but did not warrant having their own entry on the website. You can send us such notes if you want them published in the next issue.

In 2021, several people were arrested in France following the arson of vehicles belonging to Enedis (responsible for managing the electricity distribution network in France), and of an important relay antenna. A text in French details the interesting range of surveillance techniques that preceded their arrests: tailing, taking DNA from a car handle while its owner was shopping, entering a home at night to install a keylogger on a computer, asking Enedis to provide the list of people who refused installation of the new ”smart” electricity meter that they are installing everywhere, and asking a local journal to provide the IP addresses that accessed their article on the arson.

In 2022, two anarchists were arrested in Italy and charged with fabrication and possession of explosive material. A text explains that the investigation that led to the arrests started when an ”unknown person” found explosive material, electrical material and other devices in a forest in June 2021. Afterwards, the cops set up photo/video traps to ”catch” anyone who went near the area. Subsequently a person was photographed from behind near the spot, and the police subsequently alleged to have recognized and identified them.

To end this section, here's a hopeful quote from a communique claiming responsibility for the arson of a prison construction office in Germany:

> In order not to produce good pictures on the surveillance cameras, we wore rain ponchos to disguise our body shape and gait. To make our head shape unrecognizable, we used hats. The further development of