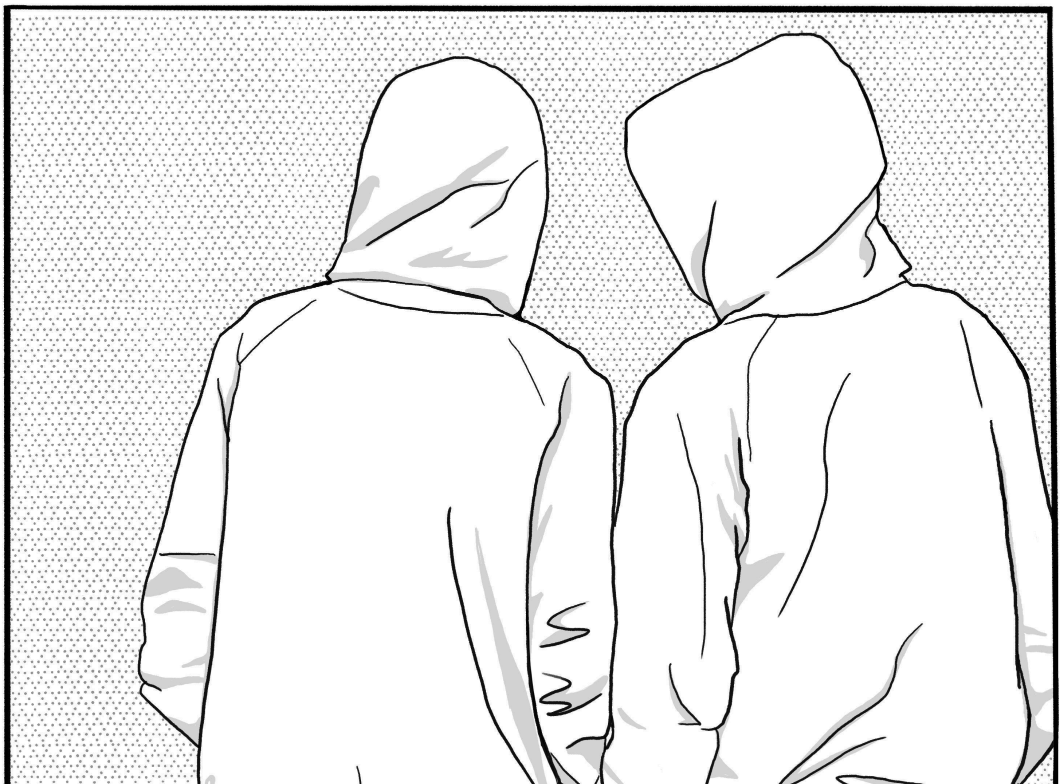
Threat Library



Threat Library

Original publication by the No Trace Project

notrace.how/threat-library

February 16, 2024

A summary of updates since this date is available at:
notrace.how/threat-library/changelog.html

Contents

1. About the Threat Library

> 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[1] detailing the surveillance that led to their arrests, 2013*

1.1. What is Threat Modeling?

Threat modeling is a conceptual exercise designed to help you identify threats, how you might be vulnerable to those threats, and what mitigations might sufficiently protect you without interfering with your ability to achieve your goals. This exercise is best done in the context of a specific project, collaboratively with the comrades you'll be working with, in **outdoor and device-free conversations (p. 69)**.

1.2. What is the Threat Library?

A prerequisite for threat modeling is an understanding of adversary behavior. The Threat Library is a knowledge base of **techniques (p. 19)** used by the enemies of anarchists and other rebels —a breakdown and classification of actions that can be used against us. These techniques are organized into a set of **tactics (p. 17)** to provide context for the technique.

Tactics represent the "*why*" of a technique, the reason for performing an action. A state adversary has three distinct but potentially overlapping tactics:

- Deterrence ("The adversary is trying to prevent you from achieving your objectives")
- Incrimination ("The adversary is trying to link you to an illegal activity")
- Arrest ("The adversary is trying to arrest you")

Techniques represent "*how*" an adversary achieves a tactical objective by performing an action. For example, an adversary may install covert surveillance devices that can later be used for incrimination.

These techniques are linked to specific **repressive operations (p. 76)** that are known to have used them, which also provides insight into the context of different **countries (p. 85)**. Each technique is paired with potential **mitigations (p. 54)** that you can take, which can help to render the technique ineffective.

Ultimately, the Threat Library is a tool to help you think through what mitigations to take on a given project, and a way to navigate resources that cover these topics in more depth. In other words, it helps you achieve the appropriate operational security[2] for your threat model.

Centralized information about repressive techniques can have a paralyzing effect; by collecting every possible approach available to our adversaries, it can make the police seem all powerful.

[1] https://notrace.how/resources/#keimeno-ton-prophulakismenon-tes-neas-philadelpheias

[2] https://notrace.how/resources/read/csrc-bulletin-1-en.html#header-a-base-to-stand-on-distinguishing-opsec-and-security-culture

The intent of the Threat Library is not to minimize or exaggerate the repressive capabilities of the State, but rather to understand its options and, more importantly, how those options are used in different contexts.

It should be emphasized that the vast majority of anarchist attacks are not successfully prosecuted. Operational security can impede the progress of investigations, even when they have a lot of resources or in contexts with a relatively small anarchist space. For example, frustrated investigators in Bremen (Germany)[3] and Grenoble (France)[4] have spoken to the media about their failure to repress any of the arson attacks that have taken place in both locations over the years, which they attribute to the **mitigations (p. 54)** taken by the arsonists.

1.3. Limitations of the Threat Library

The Threat Library is, by design, a very technical approach to anti-repression—threat modeling is done at the level of actions, and thus does not attempt to contribute to the social question; how to escape the enclosure that repression seeks, how to intervene in social tensions, and so on. While we need to develop the means to minimize the likelihood of imprisonment, struggles for freedom are not primarily a technical affair but a social one.

Such a technical approach should not lead us to overlook the psychological and emotional aspects of our struggles and our lives. As much as possible, we advise our readers to take time before, during and after an action to discuss with all comrades involved and make sure that everyone's emotional needs are taken into account.

Although the Threat Library attempts to cover as comprehensively as possible the dangers anarchists may face in their struggles, it is meant to grow with contributions over time and will never be complete. This is especially true as our enemies may evolve with new and unforeseen techniques. Thus, to avoid a false sense of security from using the Threat Library, we encourage our readers to use other sources of knowledge, to remain critical, and to always consider their personal context when making important decisions.

[3] https://notrace.how/resources/#die-sind-doch-nicht-dumm-die-nehmen-ihr-handy-naturlich-nicht-mit

[4] https://actforfree.noblogs.org/post/2022/04/17/grenoblefrance-these-saboteurs-of-the-ultra-left-have-been-elusive-for-five-years

2. Tutorial: Suggested Use of the Threat Library with Attack Trees

Attack trees are a tool to facilitate a collective brainstorming exercise on the different ways an adversary could successfully attack you in a given context, by representing the attacks in a tree structure. They help understand how a plan or project is vulnerable to repression by modeling the options available to an adversary.

This threat modeling exercise should benefit both inexperienced and experienced crews. Even if everyone already has strong security practices, this exercise provides a structured way to ensure that no threat is overlooked and that everyone is on the same page about security expectations.

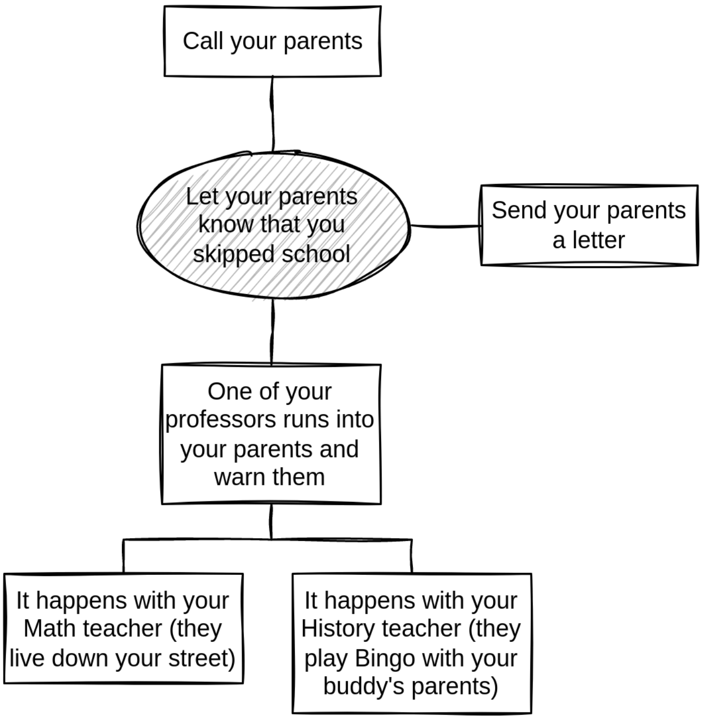
For another approach to threat modeling that can also serve as a tutorial to the Threat Library, see Threat Modeling Fundamentals[5].

2.1. A simple example: skipping a school day

Let's start with a simple example before we think about a real one. You're a kid in school, and you and your buddy want to skip a day of school, but you don't want your parents to know. The adversary is the school system.

You start by drawing the root node: it represents the adversary's goal. In this example, the goal is to let your parents know that you skipped school. The school could call your parents or send them a letter. Or one of your professors could run into your respective parents and warn them—this could happen with your Math teacher who lives down your street, or your History teacher who plays Bingo with your buddy's parents every weekend. Child nodes are different ways of getting to a parent node, and you grow the tree by identifying these children (1).

[5] https://notrace.how/resources/#threat-modeling-fundamentals


Call your parents
Let your parents know that you skipped school
Send your parents a letter
One of your professors runs into your parents and warn them
It happens with your Math teacher (they live down your street)
It happens with your History teacher (they play Bingo with your buddy's parents)

(1) “Skipping school” attack tree

Notice that the child nodes are conditions, and at least one of them must be satisfied for the immediate parent node to be true. If you can trace a path where every node is true from the furthest node on a branch to the root, the attack is complete.

So you and your buddy decide to skip a day when you don't have either Math or History. The night before you skip, you'll cut your parents' phone lines (blame it on the mice) and intercept their mail for the next few days. You're glad you came up with a great plan.

2.2. A real example: a riot in a big city in the United States

Let's say you and some comrades are preparing for a riot in a big city in the United States. You want to do some damage, but you don't want to get caught… You turn to the Threat Library for help. You print out this zine, take a pen and paper, and meet with your comrades **outdoors and without electronic devices (p. 69)**.

The goal of the discussion: draw an *attack tree*, identify techniques and mitigations that apply to your context, and decide how to implement those mitigations. After the riot, it may be a good idea to conduct an *action review*.

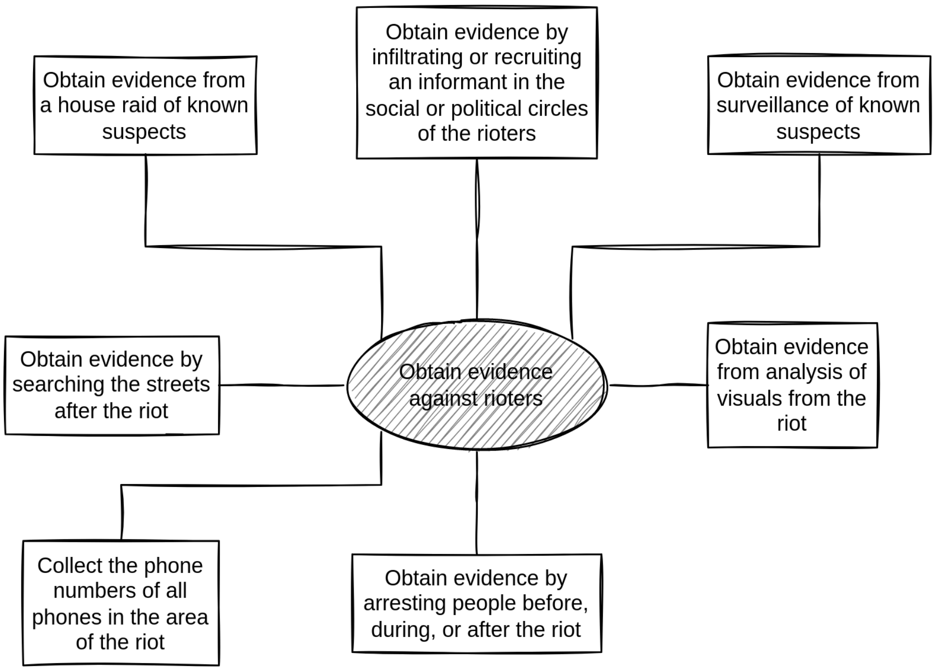
2.2.1. Draw the attack tree

In this example, the adversary is the State and its cops, and their goal is to get enough evidence of your involvement in the riots to convince a judge to convict you. You draw an attack tree to represent the ways they could achieve this goal[6]. You begin with the root node (2).

Obtain evidence against rioters

(2) "Riot" attack tree (root node)

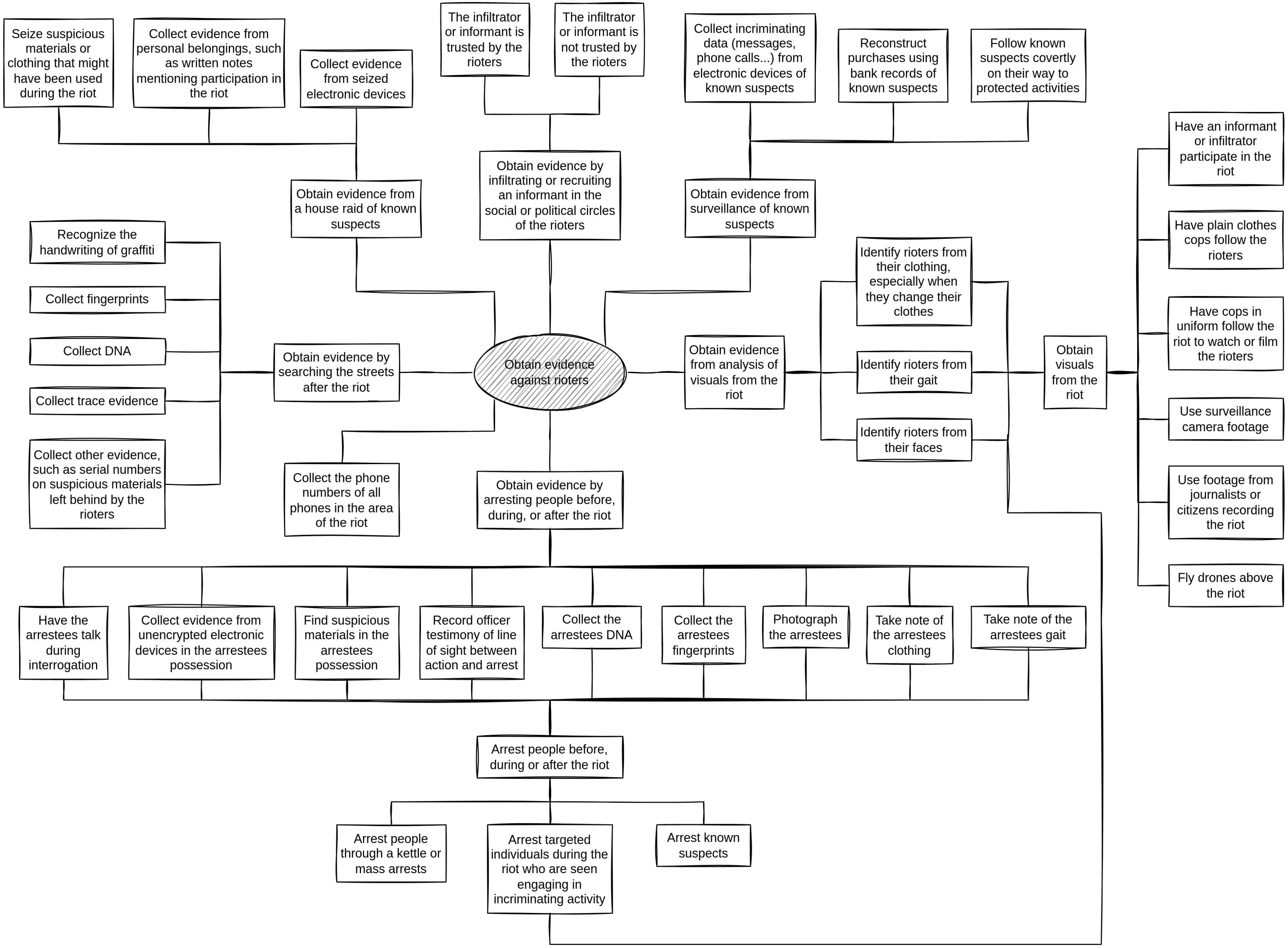
You then add the immediate child nodes, next to the root (3). At this stage, an exhaustive list of possibilities is better than a partial list of possibilities. The tree can grow in all four directions, to make it more compact.


Obtain evidence from a house raid of known suspects
Obtain evidence by infiltrating or recruiting an informant in the social or political circles of the rioters
Obtain evidence from surveillance of known suspects
Obtain evidence by searching the streets after the riot
Obtain evidence against rioters
Obtain evidence from analysis of visuals from the riot
Collect the phone numbers of all phones in the area of the riot
Obtain evidence by arresting people before, during, or after the riot

(3) "Riot" attack tree (first nodes)

You use the Threat Library to help grow the tree—reading about techniques helps you better understand all the options available to your adversary. Creating attack trees requires a certain mindset and takes practice. The tree is complete when no more substeps are needed to complete an action, and every attack that you can think of is represented (4).

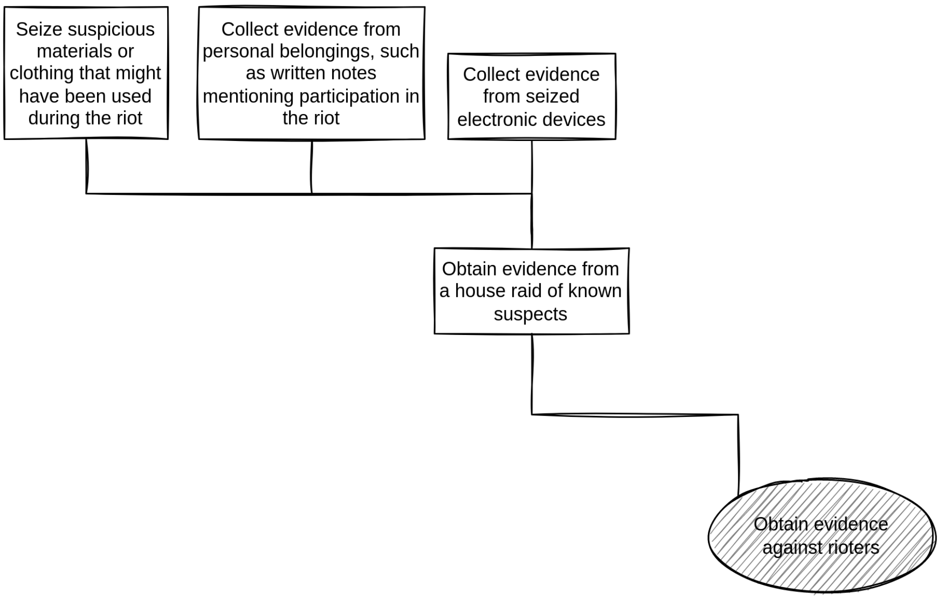
[6] For complex actions, you may want to make a temporal distinction and draw an attack tree for each step of the action (e.g. planning, preparation, execution, dissolution).


Seize suspicious materials or clothing that might have been used during the riot
Collect evidence from personal belongings, such as written notes mentioning participation in the riot
Collect evidence from seized electronic devices
The infiltrator or informant is trusted by the rioters
The infiltrator or informant is not trusted by the rioters
Collect incriminating data (messages, phone calls...) from electronic devices of known suspects
Reconstruct purchases using bank records of known suspects
Follow known suspects covertly on their way to protected activities
Obtain evidence from a house raid of known suspects
Obtain evidence by infiltrating or recruiting an informant in the social or political circles of the rioters
Obtain evidence from surveillance of known suspects
Have an informant or infiltrator participate in the riot
Recognize the handwriting of graffiti
Have plain clothes cops follow the rioters
Identify rioters from their clothing, especially when they change their clothes
Collect fingerprints
Collect DNA
Have cops in uniform follow the riot to watch or film the rioters
Obtain evidence by searching the streets after the riot
Obtain evidence against rioters
Obtain evidence from analysis of visuals from the riot
Identify rioters from their gait
Obtain visuals from the riot
Collect trace evidence
Use surveillance camera footage
Identify rioters from their faces
Collect other evidence, such as serial numbers on suspicious materials left behind by the rioters
Collect the phone numbers of all phones in the area of the riot
Obtain evidence by arresting people before, during, or after the riot
Use footage from journalists or citizens recording the riot
Fly drones above the riot
Have the arrestees talk during interrogation
Collect evidence from unencrypted electronic devices in the arrestees possession
Find suspicious materials in the arrestees possession
Record officer testimony of line of sight between action and arrest
Collect the arrestees DNA
Collect the arrestees fingerprints
Photograph the arrestees
Take note of the arrestees clothing
Take note of the arrestees gait
Arrest people before, during or after the riot
Arrest people through a kettle or mass arrests
Arrest targeted individuals during the riot who are seen engaging in incriminating activity
Arrest known suspects

(4) “Riot” attack tree (complete)

2.2.2. Identify techniques

You identify all techniques represented in the tree by matching tree nodes with techniques from the Threat Library. You do so branch by branch to avoid getting lost: it's best to start with nodes closer to the root node, and then work your way up the branch.


Seize suspicious materials or clothing that might have been used during the riot
Collect evidence from personal belongings, such as written notes mentioning participation in the riot
Collect evidence from seized electronic devices
Obtain evidence from a house raid of known suspects
Obtain evidence against rioters

(5) "Riot" attack tree (house raid branch)

You start with the "Obtain evidence from a house raid of known suspects" branch (5):

- "Obtain evidence from a house raid of known suspects" matches **House raid (p. 34)**.
- "Collect evidence from seized electronic devices" matches **Targeted digital surveillance: Physical access (p. 53)** because they would access your electronic devices, and **Targeted digital surveillance: Authentication bypass (p. 49)**, if they try to guess your passwords or break your encryption.
- The other nodes don't match anything, they're just part of the house raid.

At this stage, it can be useful to assess the risks of the techniques you're listing—this will inform whether and how thoroughly you should mitigate each of them. See the "Assessing Risk" section below for how to assess a technique's risk using the concepts of *likelihood* and *impact*.

Then you move on to the next branch until the whole tree is covered, building a table (6).

Technique	Mitigations	Implementations
House raid (medium risk)		
Physical access (medium risk)		
Authentication bypass (low risk)		

(6) Beginning of the table.

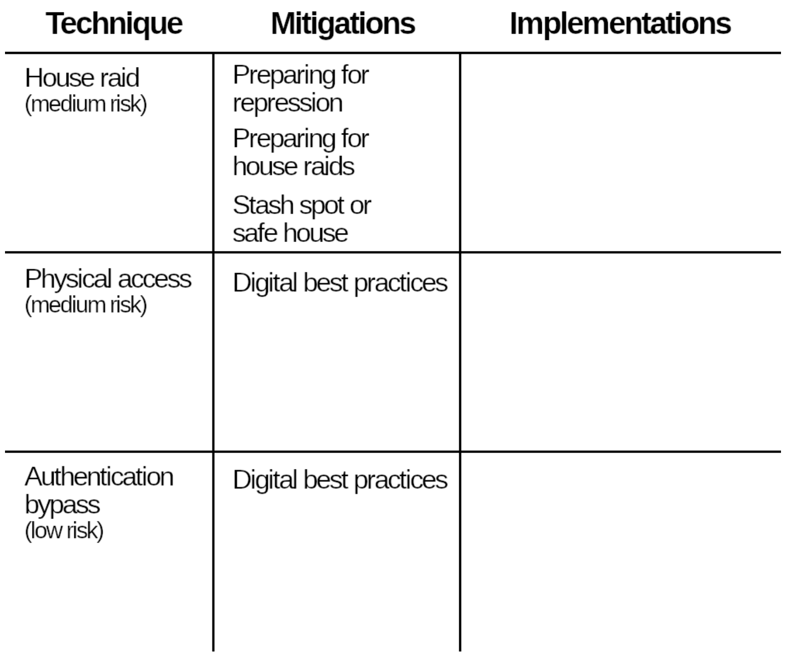
2.2.3. Identify mitigations

Next, you identify all the mitigations that you want to implement by looking at the mitigations that the Threat Library suggests for the techniques listed in the previous step.

On our example branch (5), you decide to implement:

- For “House raid”, **Preparing for repression (p. 71)**, **Preparing for house raids (p. 70)** and **Stash spot or safe house (p. 72)**. You don't want to implement **Clandestinity (p. 61)** because you decide against going down that road.
- For the two “Targeted digital surveillance” techniques, **Digital best practices (p. 63)** is the only mitigation that makes sense in your context.

You update your table (7).



Technique	Mitigations	Implementations
House raid (medium risk)	Preparing for repression Preparing for house raids Stash spot or safe house	
Physical access (medium risk)	Digital best practices	
Authentication bypass (low risk)	Digital best practices	

(7) Beginning of the table, with mitigations.

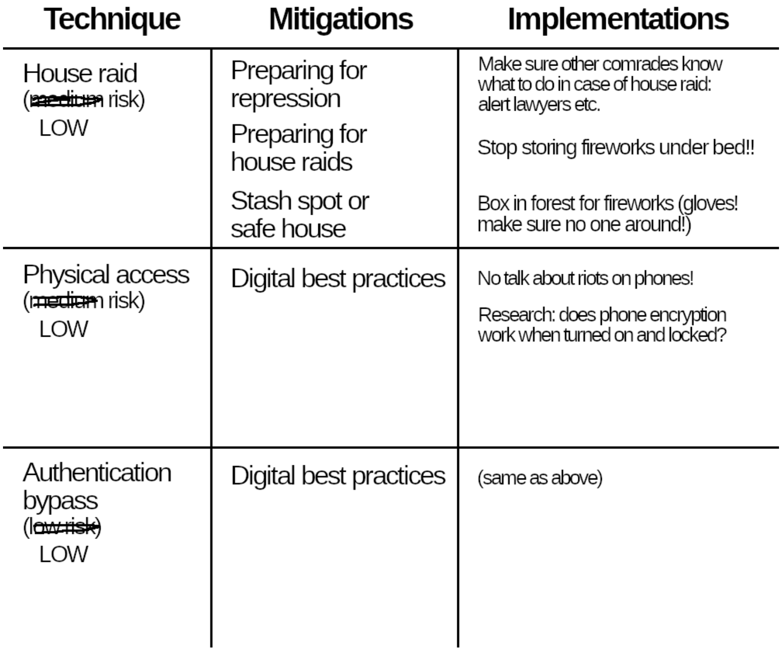
2.2.4. Decide how to implement mitigations

Finally, you decide how to implement the mitigations you have identified. Reading their entries in the Threat Library can give you some ideas. The risk you assessed for each technique helps you to know how much energy to put into the mitigations. You decide on the following implementations:

- “Preparing for repression”: since you and your comrades all live in the same place, there is a risk that you will all be arrested after a house raid. You will make sure that other comrades know how to support you if this happens.
- “Preparing for house raids”: you decide to stop storing the fireworks under your bed.
- “Stash spot or safe house”: you decide to bury a waterproof container in a nearby forest to store the fireworks. When one of you accesses it, they must wear gloves and make sure there's no one around.
- “Digital best practices”: your devices are already encrypted, and you're not using them to talk about the riots anyway. You have to find out if a phone's encryption works when it's turned on and locked because you're not sure.

At this stage, it can be useful to re-assess the risks of the techniques to make sure that they have been sufficiently lowered by the mitigations you have decided to implement.

You update your table (8).



Technique	Mitigations	Implementations
House raid (~~medium~~ risk) LOW	Preparing for repression Preparing for house raids Stash spot or safe house	Make sure other comrades know what to do in case of house raid: alert lawyers etc. Stop storing fireworks under bed!! Box in forest for fireworks (gloves! make sure no one around!)
Physical access (~~medium~~ risk) LOW	Digital best practices	No talk about riots on phones! Research: does phone encryption work when turned on and locked?
Authentication bypass (~~low risk~~) LOW	Digital best practices	(same as above)

(8) Beginning of the table, with mitigations and their implementations.

2.2.5. Burn or digitize your notes

The notes taken during this threat modeling exercise should not be kept around because they could be considered evidence of conspiracy. You have two options:

1. At the end of the exercise, memorize the findings and then burn the notes. This approach makes it difficult to later revisit your findings and expand them.
2. At the end of the exercise, digitize your notes by manually copying them to an encrypted USB device using Tails[7] and following **digital best practices (p. 63)**. These notes would be just as incriminating as a communique claiming a sensitive action, so should be treated similarly. You can use Libreoffice Draw (included in Tails by default) to draw the attack tree. Once the notes are digitized, they shouldn't be printed out because this could leave a trace on the printer, but they can be manually copied to paper again so you can revisit them away from a computer.

2.2.6. Perform an action review

After the riot, you and your comrades take some time to conduct an action review: in **outdoor and device-free conversations (p. 69)**, you discuss what went well and what went wrong, and whether there is room for improvement in the coverage of your attack tree or how you implemented the mitigations.

2.3. Assessing risk

Risk is the combined measure of a technique's impact and likelihood. If a technique would have a high impact, but is very unlikely to be used, it might be considered low risk. If a technique would have a medium impact, but is likely to be used, it might be considered high risk. If you

[7] https://tails.net

consider the risk of a technique to be high, it means that you should apply mitigations for it more thoroughly.

For example, in most contexts, the **Forensics: DNA (p. 27)** technique can be considered high risk in the threat model for an arson attack: there is both a high impact and high likelihood.

2.3.1. Impact

Impact is a measure of the consequences if a technique is used. It depends on the tactic:

- Deterrence tactic: Impact is determined by whether the target is successfully deterred.
- Incrimination tactic: Impact is determined by how "solid" the evidence gathered is.
- Arrest tactic: Impact is determined by whether the target is successfully apprehended.

Take for example DNA forensics used in an investigation into an arson, for incrimination. If the technique is used and no mitigations have been taken, a sample on a crime scene can be recovered that provides a good match to a suspect. The impact is high, as a good DNA match to an arson crime scene is solid evidence in court.

2.3.2. Likelihood

Likelihood is a measure of how likely it is that an adversary will attempt a technique.

2.3.3. Adversary resources increase risk

If more resources are devoted to the repression of an action, a given technique may be more likely to be used, increasing its *likelihood*, and be used more thoroughly, increasing its potential *impact*.

Broadly speaking, more resources are devoted to the repression of an action if the State feels more threatened by it. Actions that can be classified as "terrorism" or "threats to national security" will receive an extraordinary amount of resources in most contexts. For example, the State may devote many resources to actions that took place during an uprising, because the unrest was seen as a threat to the integrity of the State.

For example, in most countries, DNA forensics is systematically used in arson investigations. If the adversary has limited resources, the search might be limited to obvious surfaces such as door handles. If the adversary has more resources—which can be the case if the arson caused a lot of damage—the crime scene is more likely to be extensively searched for DNA evidence.

2.3.4. Mitigations decrease risk

By taking appropriate mitigations, you become less vulnerable to a technique, decreasing its potential *impact*.

For example, everyone is vulnerable to DNA forensics by default because our bodies constantly shed DNA. By applying proper **DNA minimization protocols (p. 62)** when committing an arson, you become less vulnerable to DNA forensics.

2.3.5. Risk and local context

Understanding the habits and motivations of the State agencies likely to be involved in repressing an action can help you to infer the range of repressive techniques they are likely to use, and how thoroughly they will use them. The **repressive operations (p. 76)** can help you gain an understanding of how a given technique is used in a given context.

2.4. Additional tips on using the Threat Library

The Threat Library home page[8] provides an overview of all tactics and techniques, as well as buttons that allow you to hide or show specific techniques. For example, you might want to show only techniques that fit your threat model to better visualize the techniques that might apply to your context. If you follow our suggested process above and draw your own attack trees, the overview can help you think of relevant techniques that are missing from your tree.

The Threat Library welcomes external contributions, such as:

- Changes to existing techniques, mitigations or repressive operations.
- Suggesting the addition of new techniques, mitigations or repressive operations that you think should be covered.
- Attack trees for different types of projects.
- Translating the Threat Library to new languages.

See the **contribute section (p. 87)** for more information.

[8] https://notrace.how/threat-library

3. Tactics

3.1. Deterrence

Uses techniques:

Door knocks (p. 23)
Extra-legal violence (p. 25)
Increased police presence (p. 35)
Mass surveillance (p. 39)
Police patrols (p. 47)

In some contexts, in addition to or instead of other tactics an adversary may attempt to prevent or discourage you from achieving your goals. This can be because they are unable or unwilling to incriminate or arrest you, or because they believe that discouraging you is a good complementary strategy. We call this process *deterrence*.

3.2. Incrimination

Uses techniques:

Canine trackers (p. 19)
Covert house search (p. 20)
Covert surveillance devices (p. 20)
Door knocks (p. 23)
Evidence fabrication (p. 24)
Extra-legal violence (p. 25)
Forensics (p. 26)
House raid (p. 34)
ID checks (p. 35)
Infiltrators (p. 36)
Informants (p. 37)
International cooperation (p. 38)
Interrogation techniques (p. 38)
Mass surveillance (p. 39)
Network mapping (p. 42)
Open-source intelligence (p. 43)
Parallel construction (p. 43)
Physical surveillance (p. 43)
Police patrols (p. 47)
Service provider collaboration (p. 47)
Targeted digital surveillance (p. 49)

In order to arrest you and remove you from society—usually through imprisonment—an adversary may need to convince a judge of your illicit activities. To this end, the relevant authorities will attempt to find evidence of these activites. Depending on the context and people involved, judges may be more or less easy to convince. We call this process *incrimination*.

3.3. Arrest

Uses techniques:

- **Alarm systems (p. 19)**
- **Canine trackers (p. 19)**
- **Guards (p. 33)**
- **House raid (p. 34)**
- **ID checks (p. 35)**
- **Increased police presence (p. 35)**
- **International cooperation (p. 38)**
- **Police patrols (p. 47)**

In order to remove you from society—usually through imprisonment—an adversary must be able to locate you physically and arrest you.

4. Techniques

4.1. Alarm systems

Used in tactics: **Arrest (p. 18)**

Alarm systems protect buildings and other physical or digital infrastructure by sending an alert signal when unauthorized access is detected. The alert signal can lead to the rapid intervention of a security team or law enforcement in order to investigate the situation.

For physical infrastructure, modern alarm systems will typically include sensors to detect unauthorized access to an area outside of normal operating hours. Sensors include infrared motion detectors, sensors that detect the opening of doors, and many other types of sensors[9]. The alert signal can be sent over a wired or wireless connection—low-cost modern systems often send the signal over the cellular network.

For digital infrastructure, intrusion detection systems[10] monitor for any activity that might indicate a hack is in progress. An incident response team is notified to attempt to contain and remediate any compromise.

Mitigations

Attack (p. 57): Alarm systems—or the communication lines they use to send alert signals—can be destroyed before or during an action. Wireless alert signals can also be jammed with a jamming device.

Note however that some alarm systems operate by sending signals periodically or continuously, even when nothing abnormal is detected. In such cases, destroying the alarm system will cause its signal to be interrupted, which may be interpreted as an alert and trigger an intervention.

Digital best practices (p. 63): When carrying out a cyber action, you can use defense evasion techniques[11] to prevent intrusion detection systems from detecting the action.

Reconnaissance (p. 72): Before an action, you can survey the target building or infrastructure to determine the presence of an alarm system, and the type and location of sensors or other alarm devices.

4.2. Canine trackers

Used in tactics: **Arrest (p. 18), Incrimination (p. 17)**

An adversary can bring specially trained dogs—a canine unit—to an action site and have them follow a scent. If the dogs are successful in tracking your scent, this could give the adversary clues as to the route you took out of the action site or even lead to your location. It is easier for dogs to follow a scent in rural areas than in urban areas with higher population densities.

Mitigations

Careful action planning (p. 60): If there is a possibility that a canine unit will be deployed after an action, you can plan to cross a river or use pepper spray during your exit. Bodies of water can

[9] https://en.wikipedia.org/wiki/Security_alarm#Sensor_types

[10] https://en.wikipedia.org/wiki/Intrusion_detection_system

[11] https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques

break the scent trail that the dogs are following, and pepper spray on the trail can temporarily put the dogs out of commission.

4.3. Covert house search

Used in tactics: **Incrimination (p. 17)**

A covert house search is when an adversary conducts a discreet search of a residence when the occupants are not present. This can be an opportunity for them to gather information or install **covert surveillance devices (p. 20)**.

If the area being searched has locked doors, a covert method of entry is required, such as picking the locks or asking the building owner for cooperation. Often the adversary does not want the occupants to know that the operation has taken place so they refrain from seizing materials or moving things.

In addition, the adversary can covertly seize garbage from outside a house with less effort, in the hope of finding written notes or forensic traces such as DNA traces.

Mitigations

Clandestinity (p. 61): In order to carry out a covert house search, an adversary needs to know where you live. If you take the path of clandestinity, they won't know where you live, so a search is less likely.

Physical intrusion detection (p. 70): A covert house search can be detected with the proper preparation.

Preparing for house raids (p. 70): You can prepare for a covert house search by minimizing the presence of materials that could be harmful in the event of a search.

Stash spot or safe house (p. 72): Action materials without a "legitimate" purpose should be kept in a stash spot or safe house, or at worst, should only pass through your house for a very limited time.

4.4. Covert surveillance devices

Used in tactics: **Incrimination (p. 17)**

An adversary can hide electronic devices in a variety of ways to enable data collection that would not be possible without them. They can be installed in homes, in/on a car, in a building across the street to record the comings and goings of a target's home, and even on a tree in a forest. Such an installation is usually done by a technician accompanied by surveillance operators.

They can be installed for long-term surveillance, remaining in place for weeks, months, or years before being removed by their installers—or, in some cases, found by the people under surveillance. They can also be installed for short-term surveillance of specific events.

The data collected is often transmitted over the cellular network using a SIM card included in the device, but other transmission methods are possible, such as WiFi, Bluetooth, or transmission over arbitrary radio frequencies. Some devices never transmit the data they collect and require physical access to retrieve the data.

The State often legally justifies the installation of covert surveillance devices by arguing that the target's mitigation practices (such as never **self-incriminating (p. 57)** over digital communications) make other repressive techniques ineffective.

See Ears and Eyes[12] and the hidden devices topic[13].

4.4.1. Audio

An adversary can install microphones anywhere within range of where conversations might occur—a living room, a car dashboard, a regular outdoor meeting place, etc. They can be very sensitive and successfully pick up conversations even when there is loud music playing in the background or people are whispering.

Covert microphones can be extremely small—just a few millimeters—especially if they record locally (e.g. on an SD card) and do not transmit their recordings.

Recorded conversations can be used as evidence in court if incriminating matters are discussed, or if they can be misconstrued to appear incriminating in the eyes of a judge. Non-incriminating, mundane conversations can reveal a great deal about the targets of surveillance and help in **network mapping (p. 42)**.

See Ears and Eyes[12] and the hidden devices topic[13].

Mitigations

Bug search (p. 59): With the proper techniques and tools, you can locate hidden microphones, and eventually remove them.

Outdoor and device-free conversations (p. 69): To avoid being picked up by hidden microphones, sensitive conversations should not take place indoors, in cars, or at habitual outdoor locations.

Physical intrusion detection (p. 70): Installing hidden microphones in a space often requires an adversary to covertly enter the space. With proper preparation, you can detect such a covert entry.

Repressive operations

Renata (p. 81): Six hidden microphones and a camera were found in a house after the operation[14]. The microphones were found in the living room, hallway, and bedrooms. The camera was found in the intercom system.

See the corresponding Ears and Eyes case[15].

Scintilla (p. 81): A microphone hidden in a squat for two and a half years recorded conversations that were used by the investigators to prove that the accused comrades knew each other, talked together regularly, worried about the creation of a DNA database and the impossibility of resisting DNA collection, discussed writing a text to be published[16].

See the corresponding Ears and Eyes case[17].

4.4.2. Location

[12] https://notrace.how/earsandeyes

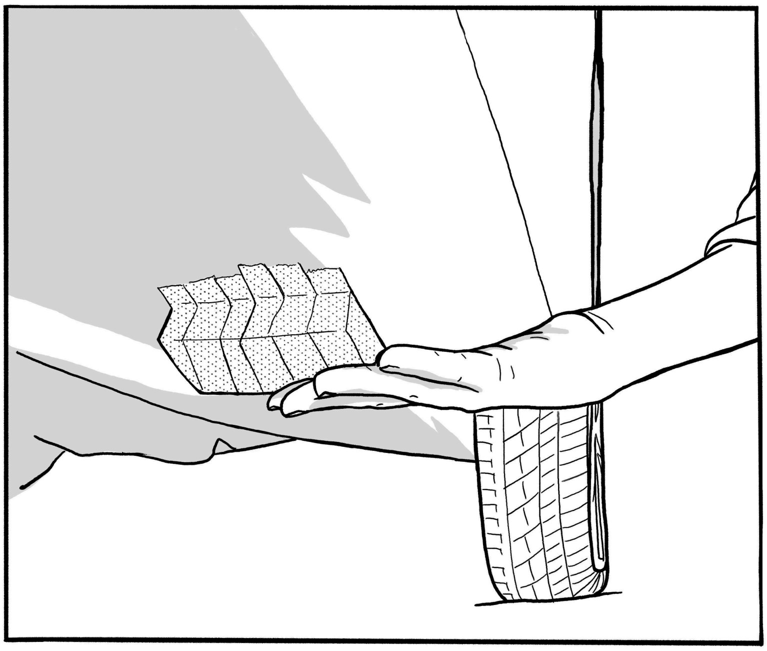
[13] https://notrace.how/resources/#topic=hidden-devices

[14] https://roundrobin.info/2019/03/trento-sei-microspie-e-una-telecamera-immagini-pesanti

[15] https://notrace.how/earsandeyes/#trento-2019-03

[16] https://macerie.org/index.php/2019/03/12/le-orecchie-della-pedrotta

[17] https://notrace.how/earsandeyes/#torino-2019-03



Location tracking devices are typically installed on the target's usual means of transportation, such as a car or bike. They often use GPS to determine their own location, but alternatives such as GLONASS or satellite phone services are also possible.

An older method used by these devices was to obtain their own location by transmitting radio waves that were received by a nearby operator (for example, in a vehicle following the target's vehicle), but this is rarely used today.

See Ears and Eyes[12] and the hidden devices topic[13].

Mitigations

Bug search (p. 59): With the proper techniques and tools, you can locate location tracking devices, and eventually remove them.

Physical intrusion detection (p. 70): Installing location tracking devices on a vehicle parked in a space often requires an adversary to covertly enter the space. With proper preparation, you can detect such a covert entry.

Transportation by bike (p. 75): Location tracking devices can be installed on bikes. However, unlike other vehicles, when **searching (p. 59)** a bike, you can determine with a high degree of confidence whether or not a tracking device is present. Bikes should be stored indoors to make it more difficult for an adversary to install a tracking device.

Repressive operations

Case against Boris (p. 77): GPS tracking devices were placed under several vehicles after investigators learned that Boris—who did not have a driver license—was being transported in them[18].

In one case, investigators learned at 2:30 p.m. from an intercepted phone call that someone close to Boris was planning to borrow a vehicle and drive Boris to a party in the evening. They witnessed the vehicle being borrowed, followed it to the party, waited until it parked, and at 9:45 p.m. they had placed a tracking device on it.

[18] https://rupture.noblogs.org/post/2023/10/04/no-bars

4.4.3. Video

An adversary can install cameras anywhere with a line of sight to the target—a front entrance to a home or social center, a motion-activated hunt cam in a tree aimed at a forest **stash spot (p. 72)**, in a living room to see what a target takes out of their bag even as they are being careful not to speak indoors, etc.

Captured images can be used as evidence in court. Non-incriminating, mundane images can reveal a lot about the targets of surveillance and help in **network mapping (p. 42)**.

See Ears and Eyes[12] and the hidden devices topic[13].

Mitigations

Bug search (p. 59): With the proper techniques and tools, you can locate hidden cameras, and eventually remove them.

Digital best practices (p. 63): Hidden cameras can film a computer or phone screen, or a computer keyboard. When using a computer or phone for sensitive activities, keep the device facing a wall that can be thoroughly searched for hidden cameras (rather than a window or TV, for example).

Physical intrusion detection (p. 70): Installing hidden cameras in a space often requires an adversary to covertly enter the space. With proper preparation, you can detect such a covert entry.

Stash spot or safe house (p. 72): By keeping incriminating materials at a stash spot or safe house, you're not bringing them into your house, where hidden cameras are more likely to be present.

Surveillance detection (p. 73): A specific passive surveillance detection technique can help you detect a surveillance vehicle parked near your home and equipped with a camera pointed at your home. This technique only works if you live in a place where there aren't too many different vehicles that park, that is, in some residential areas in cities and in most rural areas. Each time you leave or enter your home, you take note of all the vehicles parked on the street that have a line of sight to your home. Trying not to look suspicious, you note their model, color, and license plate number, either remembering the information or writing it down. After doing this for a while, you will become familiar with the “baseline” of vehicles that park on your street, which will be the vehicles of people who live nearby or their guests. Once you're familiar with the baseline, you'll be able to spot vehicles that are not part of that baseline and discreetly examine them to see if they are surveillance vehicles.

Repressive operations

Case against Boris (p. 77): Cameras were installed in the streets outside Boris's home and outside the home of someone close to him to film the entrances to the homes[18].

4.5. Door knocks

Used in tactics: **Deterrence (p. 17), Incrimination (p. 17)**

Door knocks are when an adversary comes knocking where you live to intimidate you or get information. The aim is to intimidate or create paranoia, to see who is willing to talk and possibly be recruited as an **informant (p. 37)**, and to gather information from the people who do talk.

By logging who you call or visit immediately after they come knocking, the adversary can achieve **network mapping (p. 42)**.

In many countries, it is easier for the State to carry out door knocks than **house raids (p. 34)** because door knocks do not require a warrant or legal authorization.

Mitigations

Avoiding self-incrimination (p. 57): When an adversary comes knocking, just don't talk to them —instead, alert your networks and consider making it public.

Digital best practices (p. 63): It is more difficult for an adversary to log who you contact after they come knocking if you use digital best practices.

Repressive operations

Scintilla (p. 81): In May 2019, cops knocked on Boba's door under the pretext of giving a verbal notice to another comrade[19]. Once inside, however, they revealed a warrant for Boba's arrest, arrested him, and searched the house.

4.6. Evidence fabrication

Used in tactics: **Incrimination (p. 17)**

Evidence fabrication can include anything from lying in a police report to planting incriminating material, though this can be exposed during a trial if not done well.

For example, police in Baltimore (United States) were unaware that their body cams continued to record after being turned off and recorded themselves planting drugs in a suspect's bag. Depending on the context, such evidence fabrication can be either common or rare.

[19] https://macerie.org/index.php/2019/05/23/incendio-al-carcere-boba-arrestato

A common practice of investigators, prosecutors, and judges is to "make up a story", assembling facts and theories to fit their predetermined hypothesis about a case. This widespread strategy is one of the reasons why it is important to prevent cops from gathering any information about us, because enough information (even mundane information) can be woven into a narrative for their purposes.

Mitigations

Need-to-know principle (p. 68): Evidence fabrication is harder to achieve when an adversary has less information about our lives. The need-to-know principle controls the flow of information through networks to make them more opaque to adversaries.

Physical intrusion detection (p. 70): Planting evidence in a space often requires an adversary to covertly enter the space. With proper preparation, you can detect such a covert entry.

4.7. Extra-legal violence

Used in tactics: **Deterrence (p. 17), Incrimination (p. 17)**

The State may use physical and psychological extra-legal violence and, in some contexts, extra-legal assassination.

In Russia and Belarus, several anarchists have been tortured in recent years after being arrested by State agents. Reported acts of torture in these countries include:[20].

Mitigations

Preparing for repression (p. 71): If your context includes the risk of torture after arrest, you may want to prepare for that risk. Possible preparations include:

- Preparing psychologically.
- Setting up protocols in advance that allow a network to learn when someone is missing in order to respond quickly to their disappearance. For example, members of a group may connect to an encrypted messaging platform once a day to send each other a message: if a member does not send their daily message, it may mean they have been arrested. Torture often occurs immediately after arrest, while no one knows where the person is and there is no lawyer, so responding quickly after arrest can be crucial.
- Depending on the context, involving a lawyer or publicizing the acts of torture can help put pressure on the authorities to stop.

Repressive operations

Network (p. 80): Most of the defendants were tortured by agents of the Russian Federal Security Service (FSB) in the early stages of their detention in order to obtain (often fabricated) statements that could later be used to charge and convict them[21]. Most of the defendants who were tortured later retracted their statements and spoke publicly about the torture they had received.

Renata (p. 81): During the house raids in February 2019, one of the arrested comrades was forced to his knees by a cop who put a gun to his temple[22].

[20]

beatings, suffocation with a plastic bag or pillow, pouring water into the nose and mouth, hanging by the legs or by tied hands, electric shocks, torture with a screwdriver, forcing people to do squats until they collapse, sexual violence, and deprivation of sleep, food, and water.

[21] https://web.archive.org/web/20210724133854/https://a2day.net/network-underground

[22] https://infernourbano.altervista.org/che-si-sappia-comunicato-dal-trentino

Belarusian anarcho-partisans (p. 77): The anarchists were tortured in the first days of their detention[23].

Repression of the 2019 uprising in Chile (p. 78): In the streets and in custody, police forces and soldiers injured, sexually assaulted, raped, tortured and killed many protesters in what appeared to be a strategic attempt to deter participation in the uprising[24].

4.8. Forensics

Used in tactics: **Incrimination (p. 17)**

Forensics is the application of science to investigations for the collection, preservation, and analysis of evidence. It has a broad focus: DNA analysis, fingerprint analysis, bloodstain pattern analysis, firearms examination and ballistics, toolmark analysis, serology, toxicology, hair and fiber analysis, footwear and tire tread analysis, drug chemistry, paint and glass analysis, linguistics, digital audio, video, and photographic analysis, etc. In addition to linking a suspect's identity to an action, forensics is often used to link individual actions together.

Forensic scientists often testify as "expert witnesses" at trials.

4.8.1. Arson

Fire investigations have two distinct phases: fire scene investigation, which focuses on evidence at the scene of the fire, and fire debris analysis, which focuses on evidence removed from the scene and analyzed in a laboratory.

Fire scene investigation becomes much more difficult when the "flashover" point has been reached—when a room becomes so hot that every ignitable surface bursts into flames. This phase involves determining whether a fire was intentionally set and identifying its point of origin.

Fire debris analysis focuses on ignitable liquid residues (ILRs) and aims to identify potential traces of accelerant and their chemical composition—these samples are usually found by dogs at the scene.

Mitigations

Anonymous purchases (p. 55): Accelerants can sometimes be identified and traced back to a gas station brand, and from there, to the identity of the buyer. To prevent this, you should purchase accelerants anonymously.

Careful action planning (p. 60): Different actions can be tied together if accelerant from the same source is used in all of them. To prevent this, you should not reuse accelerant from the same source in different actions.

4.8.2. Ballistics

Forensic ballistics is the examination of evidence from firearms. When a bullet is fired from a gun, the gun leaves microscopic marks on the bullet and cartridge case. These marks are like ballistic fingerprints.

[23] https://pramen.io/en/2021/12/blood-on-your-hands-regarding-information-about-torture-of-anarcho-partisans

[24] https://es-contrainfo.espiv.net/2019/11/06/chile-una-mirada-anarquica-al-contexto-de-revuelta-y-represion

When an adversary recovers bullets from a crime scene, forensic examiners can test-fire a suspect's gun and then compare the marks on the crime scene bullet to the marks on the test-fired bullet. Cartridge cases are compared in the same way.

Mitigations

Anonymous purchases (p. 55): Purchasing firearms and ammunition anonymously is difficult, but not impossible. It usually involves connections to organized criminal networks or fraud.

Stash spot or safe house (p. 72): To perform a ballistic analysis, an adversary must have the firearm in their possession for comparison. To prevent this, you can store the firearm in a stash spot or safe house.

4.8.3. DNA

DNA is the molecule that contains the genetic code of organisms. With the exception of red blood cells, every cell in our body has DNA. We constantly shed DNA into the environment through skin cells, hair, saliva, blood, sweat, etc. DNA traces can be collected from our bodies or the environment and analyzed in specialized laboratories to reveal information about the individuals they came from.

Analysis of a DNA trace can provide basic information about the individual it came from, such as their genetic sex. Comparison of two DNA traces can determine whether they belong to the same individual, to individuals who are closely related genetically (e.g., parents and their children, cousins), or to unrelated individuals.

DNA in the environment degrades over time and under certain conditions, and a DNA trace must contain a sufficient amount of undegraded DNA to be successfully analyzed. As technology advances, this amount decreases.

In many countries, the State has DNA databases containing the genetic information of many individuals, often obtained during arrests or as part of criminal convictions. DNA is often treated in trials as the "gold standard", indisputable proof that a person was in contact with the surface where their DNA was found.

See blabladn[25] for a comprehensive overview of DNA forensics literature and the DNA topic[26].

Mitigations

Careful action planning (p. 60): Each step of an action plan can be rehearsed with an eye toward minimizing DNA traces at the site of the action. This may include, for example:

- Securing your hair under a hat.
- If you have to cut a fence, cutting any fence holes large enough to pass through without touching the fence.
- Ensuring that surfaces at the site are not touched if they do not need to be, and that surfaces that need to be interacted with (such as a door handle) are touched by someone following **DNA minimization protocols (p. 62)**.
- Ensuring that any destructive device left at the site (e.g. an incendary device with a delay) has worked as expected in tests conducted under similar conditions (temperature, etc.). The point of this is to make sure that the device will not be recovered intact by an adversary.
- Ensuring that nothing is accidentally left behind such as a bag, tool, or anything that falls out of a pocket.

[25] https://notrace.how/resources/#blabladn

[26] https://notrace.how/resources/#topic=dna

DNA minimization protocols (p. 62): If you minimize the amount of DNA you leave on an object you manipulate, you minimize the risk that DNA forensics draws any valuable conclusion from an analysis of the object.

Gloves (p. 66): You can wear gloves to prevent DNA from being left on objects you touch.

Repressive operations

Scripta Manent (p. 83): DNA evidence was used to convict Alfredo Cospito[27].

Case against Boris (p. 77): The only evidence against Boris was that his DNA was found on a bottle cap at the foot of one of the burnt antennas from the April sabotage[18].

When DNA was collected from someone close to Boris during a house raid, only eight and a half hours elapsed between the collection of the DNA trace and the result of its comparison with other traces collected earlier.

Repression against Zündlumpen (p. 78): The only clue against a suspected editor of the newspaper was that their DNA was found on a cigarette butt in the print shop raided in April 2022[28].

Renata (p. 81): After their arrest and imprisonment, the comrade accused of the explosive attack on the "Lega Nord" headquarters in Treviso refused to have their DNA taken[29]. Some time after the comrade's refusal, prison guards searched their cell and secretly replaced one comb with another, presumably to obtain the comrade's DNA from the hairs on the comb they took.

Repression of Lafarge factory sabotage (p. 76): In one of the initial raids, police insisted that those arrested wear surgical masks to protect against Covid: the masks were later taken for DNA collection[30]. One person who refused to wear a mask had their underwear confiscated while in police custody, presumably for DNA collection[31].

Prometeo (p. 80): DNA traces were used to convict the comrade accused of burning an ATM[32].

Mauvaises intentions (p. 82): During police custody, DNA was collected from the comrades' clothing and from plastic cups[33]. In one case, only nine hours elapsed between the collection of a DNA trace in custody and the result of its comparison with another trace collected earlier.

The charges against a comrade were based on a match between his DNA and DNA collected at the scene of the attempted arson of the electrical cabinet. DNA traces were collected both from a latex glove found nearby and from a bottle inside the cabinet—which did not catch fire because of a failed delay.

The charges against other comrades were based on a match between their DNA and DNA collected from a cigarette used as a delay for an incendiary device—the delay failed and the device was found intact under the police tow truck.

Repression of the first Jane's Revenge arson (p. 76): In May 2022, DNA traces were collected from several items found by investigators at the crime scene, including a broken window, a glass jar, a lighter, and an intact Molotov cocktail[34]. In March 2023, police saw the comrade who was later arrested discard a brown paper bag containing a partially eaten burrito in a public trash can. DNA traces collected from the bag's contents matched those collected at the crime scene.

[27] https://insuscettibilediravvedimento.noblogs.org/post/2020/03/29/it-en-italia-su-una-sentenza-e-qualcosa-daltro-un-testo-di-marco-dal-carcere-di-alessandria

[28] https://notrace.how/resources/#die-verfolgung-von-anarchist-innen-und-kippenstummeln-im-bajuwarisch-christlichen-konigreich

[29] https://roundrobin.info/2020/03/aggiornamenti-su-manu-stecco-juan-e-sasha

[30] https://sansnom.noblogs.org/archives/16831

[31] https://notrace.how/resources/#affaire-lafarge-les-moyens-denquetes-utilises

[32] https://roundrobin.info/2021/05/sentenza-beppe

[33] https://infokiosques.net/spip.php?article597

[34] https://notrace.how/documentation/first-jane-s-revenge-arson-investigation-files.pdf

Scintilla (p. 81): The charge against Peppe was based on a match between DNA traces found inside the parcel bomb and his DNA collected from a cigarette butt during the investigation[35].

Nea Filadelphia case (p. 82): The charges against several comrades were based on a match between their DNA, taken by force while in custody, and DNA traces found on "mobile objects" near the robberies[36].

Panico (p. 80): DNA traces were the only evidence against one of the accused comrades[37].

2019-2020 case against Mónica and Francesco (p. 78): Francesco's DNA was allegedly found on the parcel bomb sent to the former Minister of the Interior, which was defused and didn't explode[38].

4.8.4. Digital

Digital forensics is the retrieval, storage, and analysis of electronic data that can be useful in criminal investigations. This includes information from computers, hard drives, phones, and other data storage devices.

For example, digital forensics can be used to retrieve a "deleted" file from a computer's hard drive, retrieve a phone's web browsing history, or determine how a server was hacked.

Mitigations

Avoiding self-incrimination (p. 57): You should not store self-incriminating information on digital devices except for very deliberate reasons, such as writing and sending an action claim, and always through **Tails (p. 63)**.

Digital best practices (p. 63): To retrieve electronic data from a computer that has been turned off, the computer must contain traces of what it was used for. To prevent this, you can use Tails[39], an "amnesic" operating system designed to leave no trace on the computer it runs on. Tails is a forensic examiner's worst nightmare.

When investigating cyber actions, forensic methods are used to analyze the targets of the hack to determine where the attack came from (attribution)—this may include determining what tools were used and any other "signatures". The use of popular rather than custom tools can help prevent attribution. If attribution is possible, discrete hacks can be linked together. Implementing operational security during the hack will get in the way of deanonymization—any Virtual Private Servers (VPSs) used should be **purchased anonymously (p. 55)** and accessed only through Tails[39].

Encryption (p. 65): Electronic data retrieved from a digital device is useless if it is encrypted and cannot be decrypted by the forensic examiner. To achieve this, you can encrypt your devices with Full Disk Encryption and a strong password. This type of encryption is only active when the device is completely powered down (not locked or hibernating), so all your encrypted devices should be turned off when not in use.

Metadata erasure and resistance (p. 67): Metadata can be retrieved by digital forensics like any other data. To prevent this, metadata should be deleted before a file is published online or sent to others.

[35] https://roundrobin.info/2019/12/verona-una-perquisizione-e-un-arresto

[36] https://abcsolidaritycell.espivblogs.net/archives/130

[37] https://panicoanarchico.noblogs.org

[38] https://notrace.how/resources/#uber-orwell-und-der-fall-von-monica-und-francisco

[39] https://tails.boum.org

4.8.5. Facial recognition

Facial recognition is a technology that can match a human face from a digital image or video against a database of faces.

It works by locating and measuring facial features from a given image—today, sophisticated facial recognition technology is capable of identifying a masked individual if their eyes and eyebrows are visible. Facial recognition, coupled with **mass video surveillance (p. 40)**, is used to automate the tracking of identified individuals through a space. There is no consensus on its use as evidence in court.

See the facial recognition topic[40].

Mitigations

Anonymous dress (p. 54): You can wear a wear a mask that adequately covers your face, including your eyebrows and up to the top of your nose.

Biometric concealment (p. 59): You can wear a mask to cover your facial features, and sunglasses or a hat with a low brim to cover your eyes.

Repressive operations

2019-2020 case against Mónica and Francesco (p. 78): In order to identify Mónica and Francesco on public CCTV footage, photos of both were compared to the footage, including a comparison of several facial features: eye distances, wrinkles, piercing scars, ear size, mouth and nose shape[38].

4.8.6. Fingerprints

Fingerprints are the impressions left by the ridges of our fingers. They are left on surfaces we touch by the moisture and grease on our fingers. They can also be collected from our fingers using ink or other substances (fingers are first dipped in ink, then put on paper, leaving impressions on the paper), or using electronic fingerprint scanners. Because fingerprints are nearly unique and durable over the life of an individual, two fingerprints can be compared to determine if they belong to the same individual.

Fingerprints left on surfaces degrade over time and under certain conditions (e.g., in contact with acetone), and must contain a sufficient amount of detail to be useful in a comparison. On some surfaces, such as metal, the reaction between the finger grease and the metal can etch a print into the surface itself, leaving the fingerprint identifiable even after the surface is wiped with an acetone-soaked cloth.

In many countries, the State has fingerprint databases containing the fingerprints of many individuals, often obtained during arrests.

See the fingerprints topic[41].

Mitigations

Careful action planning (p. 60): Any tools you plan to use during an action should be fingerprint-free in case you lose them or have to discard them in a place where they can be recovered by an adversary.

Gloves (p. 66): You can wear certain types of gloves to avoid leaving fingerprints on objects you touch.

[40] https://notrace.how/resources/#topic=facial-recognition

[41] https://notrace.how/resources/#topic=fingerprints

4.8.7. Gait recognition

Gait is the way we move, a type of behavioral biometric. Gait recognition identifies people by their walking style and pace, which are extremely difficult to change.

Each person's gait can be defined by unique measurements such as the position of the ankle, knee, and hip. Gait recognition can identify people even when their faces are obscured. Advanced gait recognition technologies can identify a person from a great distance, even if they are deliberately trying to change their gait.

Mitigations

Anonymous dress (p. 54): You can conceal your gait by wearing baggy clothing.

Biometric concealment (p. 59): You can conceal your gait by wearing baggy clothing that hides your body shape, using an umbrella or other concealing objects, or drastically changing your walking style by adopting a "funny walk".

Repressive operations

Bialystok (p. 79): The main evidence against the comrade accused of an explosive attack on a police station was a comparison of his gait and the color of his coat with the corresponding characteristics of a person recorded by the surveillance cameras of the police station[42].

Scintilla (p. 81): Two of the comrades were accused of arson because their gait and walking style were considered compatible with individuals caught on video surveillance placing a canister of flammable liquid in front of an Italian post office[43][44].

4.8.8. Handwriting analysis

Each person has a unique way of writing. Handwriting analysis is a process that relies on knowledge of the unique characteristics of letter formation and the physiological processes behind writing—the ways in which a person's fine motor skills can affect their handwriting and leave clues to the writer's identity.

Mitigations

Biometric concealment (p. 59): You can conceal your handwriting by writing on digital devices instead of by hand. When writing graffiti, use only capital letters and make the lettering as generic as possible.

Repressive operations

Scripta Manent (p. 83): Handwriting samples of some of the accused comrades (including notes seized during raids and letters written from prison) were compared to handwritten addresses on unexploded parcel bombs in an attempt to link the comrades to the attacks[45].

Repression of the first Jane's Revenge arson (p. 76): A comparison between the cursive graffiti left at the crime scene and the same style of graffiti painted a few months later during a demonstration helped identify the comrade who was later arrested[34].

2019-2020 case against Mónica and Francesco (p. 78): The sticker of the parcel bomb sent to the police station remained intact despite the explosion of the package; the address information written on the sticker was compared to Francesco's handwriting and positively matched[38].

[42] https://ilrovescio.info/2022/02/02/aggiornamento-sulle-misure-e-sul-processo-per-lop-byalistok

[43] https://macerie.org/index.php/2019/04/17/ultime-da-carceri-e-tribunali

[44] https://attaque.noblogs.org/post/2020/08/06/saint-etienne-arrestation-de-carla-recherchee-dans-le-cadre-de-loperation-scintilla

[45] https://lib.anarhija.net/library/operation-scripta-manent-in-italy-2016-2019#toc15

4.8.9. Linguistics

Forensic linguistics is used to identify the author of a text or the person behind a voice. Author identification (also called *stylometry*) is based on the analysis of certain patterns of language use: vocabulary, collocations, spelling, grammar, etc. Voice identification is based on speech sounds (*phonetics*) and the acoustic qualities of the voice.

Author identification can be used, for example, to determine:

- Who wrote an anonymous claim of responsibility posted on the Internet or sent to a newspaper.
- Whether multiple anonymous claims of responsibility were likely written by the same person or group.
- Who wrote a plan describing illegal activities found during a **house raid (p. 34)** or an arrest.

Voice identification can be used, for example, to determine:

- Who is speaking on a tapped mobile phone or a recording made by a **hidden microphone (p. 21)**.
- Who called the authorities to make a bomb threat.

On the topic of author identification, see Counteracting Forensic Linguistics[46] and Who wrote that?[47].

Mitigations

Biometric concealment (p. 59): You can conceal your voice by hiding its acoustic properties.

Masking your writing style (p. 67): You can counter author identification by masking your writing style.

Repressive operations

Scripta Manent (p. 83): Texts published by some of the accused comrades were compared with claims of responsibility by the Informal Anarchist Federation, with the aim of proving that the comrades had written these claims[45].

4.8.10. Trace evidence

Tiny fragments of physical evidence, called *trace evidence*, can be transferred between objects, or between objects and the environment. This can happen when two objects touch, or when small particles are dispersed by an action or movement. Trace evidence can be analyzed to establish links between people, objects, and places.

Examples of trace evidence include hair (including pet hair), gunshot residue, fibers from clothing, paint chips, and pieces of glass. Less common examples include soil, cosmetics, and fire debris.

See the other physical traces topic[48].

Mitigations

Anonymous dress (p. 54): By dressing anonymously, you can prevent an adversary from linking trace evidence from your clothing (e.g., textile fibers detaching from your clothing into the environment) back to you.

[46] https://anonymousplanet.org/guide.html#appendix-a4-counteracting-forensic-linguistics

[47] https://notrace.how/resources/#wer-schreibt-denn-da

[48] https://notrace.how/resources/#topic=other-physical-traces

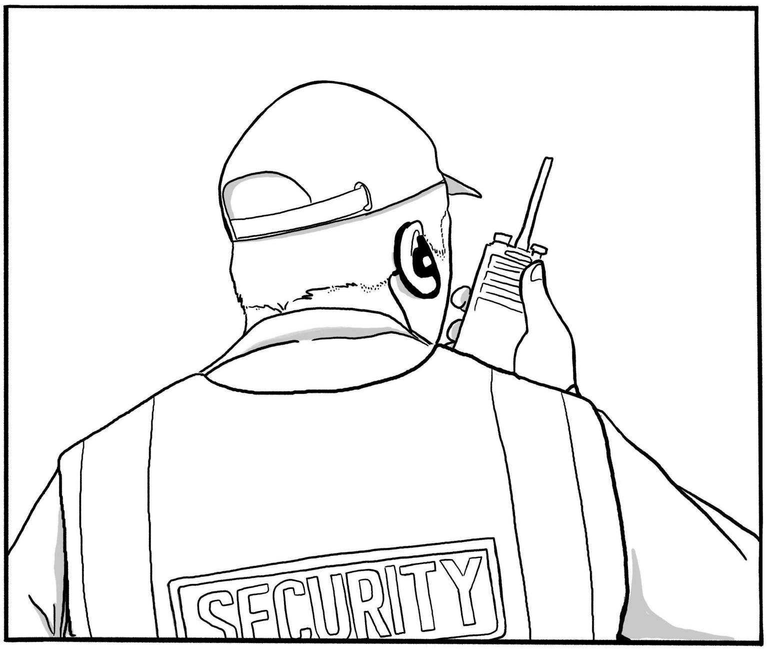
Careful action planning (p. 60): Trace evidence can link objects to an action site. To prevent this, after the action, you can plan to dispose of any tools or clothes you used during the action.

Stash spot or safe house (p. 72): Trace evidence can link objects to an action site. To prevent this, you can store in a stash spot or safe house any tools that are too expensive to realistically discard after each action.

Repressive operations

Case against Jeff Luers (p. 83): In the raid of the storage unit, the police found a bolt cutter matching the cuts in the fence surrounding the site of the May arson attempt[49].

4.9. Guards



Used in tactics: **Arrest (p. 18)**

Human guards can be hired to protect buildings or other physical infrastructure.

If they detect an unauthorized presence in the area under their watch, the guards can decide to intervene themselves or call for outside help. Depending on the context, they may be armed with lethal or non-lethal weapons.

Mitigations

Attack (p. 57): You can incapacitate guards to prevent them from interfering with an action. For example, in their attacks on logging companies machinery in so-called Chile, Mapuche people have neutralized guards by disarming them[50], tying them up[51] or shooting at them[52].

Reconnaissance (p. 72): Before an action, you can identiy the presence of guards at an action site.

[49] https://www.courtlistener.com/opinion/2627996/state-v-luers

[50] https://actforfree.noblogs.org/post/2022/08/04/chile-a-fiery-july-in-the-mapuche-territories

[51] https://actforfree.noblogs.org/post/2022/02/28/chile-the-mapuche-struggle-continues-under-a-state-of-emergency

[52] https://actforfree.noblogs.org/post/2021/07/21/chile-mapuche-zone-ignites-after-the-murder-of-pablo-marchant-update

4.10. House raid

Used in tactics: **Arrest (p. 18), Incrimination (p. 17)**

A house raid is when an adversary conducts a surprise search of a residence, sometimes accompanied by simultaneous arrests. This is often done early in the morning when the occupants are asleep and taken by surprise. However, if the goal is to obtain electronic devices when they are turned on, the timing is more likely to be during the day.

In general, all electronic devices are seized for analysis, as well as anything potentially useful for building the case or **network mapping (p. 42)** literature, materials that could be used for actions, clothing, etc.

In addition to their usual goal of finding evidence, house raids are sometimes used as an opportunity to:

- Arrest individuals.
- Disrupt the targets' ability to organize by seizing expensive items (e.g., computers, printing equipment).
- Install **covert surveillance devices (p. 20)** at the raided location.

In some countries, the State is only allowed to search the rooms of those named in a warrant.

Mitigations

Clandestinity (p. 61): In order to carry out a house raid, an adversary needs to know where you live. If you take the path of clandestinity, they won't know where you live, so a raid is less likely. Sometimes a house raid is what prompts clandestinity—charges are made public, and if the person is not at home during the raid, they may decide to avoid arrest by going into clandestinity.

Preparing for house raids (p. 70): You can prepare for a house raid by minimizing the presence of materials that could be harmful in the event of a raid.

Preparing for repression (p. 71): House raids are often accompanied by arrests—having plans in case of arrest can make a big difference.

Stash spot or safe house (p. 72): You should keep action materials without a "legitimate" purpose in a stash spot or safe house, or at worst, have them pass through your house for a very limited time.

Repressive operations

Scripta Manent (p. 83): One comrade was arrested after batteries and an electrician's manual were found in his home during a raid[53].

Renata (p. 81): During a house raid, cops tried to get into the basement before waking up the comrades in the house, then privately complained that they were unable to hide what they wanted to hide[22].

Repression of Lafarge factory sabotage (p. 76): Among the initial house raids, one was particularly thorough: the police searched under mattresses, behind sofa covers and in every drawer of every piece of furniture, inspected every book, notebook and piece of clothing as well as the dishes, and emptied packages of pasta and sealed jars[54].

Case against Jeff Luers (p. 83): During the raid of the storage unit, the police found[49]:

[53] https://web.archive.org/web/20170928080735/http://www.informa-azione.info/italia_repressione_5_nuovi_arresti_e_una_trentina_di_perquisizioni_per_attacchi_federazione_anarchica_informale

[54] https://sansnom.noblogs.org/archives/16978

- Ignition devices matching those found at the site of the May arson attempt, as well as materials used to make incendiary devices (gas cans, sponges, spools of thread, and incense sticks).
- A bolt cutter matching the cuts in the fence surrounding the site of the May arson attempt.

4.11. ID checks

Used in tactics: **Arrest (p. 18)**, **Incrimination (p. 17)**

An ID check (short for *identity check*) is the process by which the State verifies a person's identity by asking them for their personal information, requiring them to produce a government-issued ID document, or taking their biometric information (face photograph, fingerprints, DNA) and comparing it against a database. An ID check can be a pretext for questioning and pressuring, and can be followed by a search of the person's belongings.

Complying with an ID check gives the State information about you, which can help them achieve **network mapping (p. 42)**, and can lead to your arrest if you are wanted by them. The consequences of being unable or refusing to comply with an ID check are highly context-dependent, but may include having your biometric information taken by force or without your knowledge, being detained, and being deported out of the country.

The likelihood of being targeted by an ID check depends on the situation and on how you are perceived by the State. You are less likely to be targeted if you are engaged in inconspicuous activites and dressed to appear wealthy. You are more likely to be targeted if you are perceived as a potential criminal or illegal immigrant, or if you are entering or leaving a riot.

Mitigations

Avoiding self-incrimination (p. 57): If possible, do not answer questions or provide biometric information (face photograph, fingerprints, DNA) during ID checks.

Fake ID (p. 66): If providing your real identity during an ID check could lead to your arrest or other negative consequences, presenting a fake ID may be a solution, as long as the fake ID is not recognized as such by the State.

Repressive operations

Case against Boris (p. 77): Investigators obtained and analyzed records of ID checks made by local police shortly before and after the sabotages, in different perimeters around where the sabotages took place, presumably hoping to find the names of the saboteurs in those records[18].

4.12. Increased police presence

Used in tactics: **Arrest (p. 18)**, **Deterrence (p. 17)**

The police increase their presence in a particular place and time for two reasons: to intimidate, and to improve their options for intervention and their responsiveness.

Examples of increased police presence include:

- More frequent **police patrols (p. 47)** in a particular area.
- The deployment of police officers and vehicles at a public demonstration. In the hours before a demonstration begins, police officers and vehicles can cluster on the streets surrounding the demonstration or around its expected targets. This clustering can be an opportunity for them to conduct **overt surveillance (p. 46)** before, during, and after the demonstration.

Mitigations

Attack (p. 57): If an increased police presence is organized in anticipation of a public demonstration, it can be inconsequential if the crowd is large and fierce enough. Decentralized and autonomous forces are more agile than the rigid chain of command that police agencies rely on for crowd control. For example, despite years of planning to militarize Hamburg, Germany, for the G20 summit, rioters were able to liberate a neighborhood from police occupation for an entire night[55].

Careful action planning (p. 60): Police cannot be everywhere all the time, even with an increased presence in a given area. Agility, thorough **reconnaissance (p. 72)**, and a good escape plan can go a long way. For arson attacks, the use of timers can allow an attack to be carried out unobserved right under their noses. Increased police presence in one place also means the possibility of decreased police presence elsewhere.

4.13. Infiltrators

Used in tactics: **Incrimination (p. 17)**

An infiltrator is someone who infiltrates a group or network by posing as someone they are not in order to gain information or destabilize the group or network. They may come from police, intelligence or military forces, from a private company or contractor, or they may act for ideological reasons (e.g. fascists) or under duress (e.g., they are told they will be imprisoned if they don't work as an infiltrator).

Stop Hunting Sheep[56] describes five basic types of infiltrators:

1. Hang Around: Less active, attends meetings, events, collects documents, observes and listens.
2. Sleeper: Low-key at first, more active later.
3. Novice: Low political analysis, “helper”, builds trust and credibility over longer term.
4. Super Activist: Out of nowhere, now everywhere. Joins multiple groups or committees, organizer.
5. Ultra-Militant: Advocates militant actions and conflict.

Infiltration can be “shallow” or “deep”. A shallow infiltrator may have a fake ID, but is more likely to return to their normal life over the weekend. Shallow infiltration generally occurs earlier in the intelligence gathering lifecycle than deep infiltration, when targets are still being identified. In contrast, a deep undercover lives the role 24 hours a day, for extended periods of time (with periodic breaks). They may have a job, an apartment, a partner, or even a family as part of their undercover role. They will have a fake government-issued ID, employment and rental history, etc.

See the infiltrators topic[57].

Mitigations

[55] https://crimethinc.com/2017/08/07/total-policing-total-defiance-the-2017-g20-and-the-battle-of-hamburg-a-full-account-and-analysis

[56] https://notrace.how/resources/#stop-hunting-sheep

[57] https://notrace.how/resources/#topic=infiltrators-and-informants

Attack (p. 57): You can attack infiltrators when uncovered or years later[58] to discourage the practice—police infiltrators are likely to be less enthusiastic if there is a local precedent of violence against them.

Background checks (p. 58): Background checks can help ensure that someone in your network is not an infiltrator.

Need-to-know principle (p. 68): The need-to-know principle controls the flow of information through networks to make them more opaque and difficult to disrupt. If an infiltrator isn't involved in an action, they shouldn't know who was involved even if it's their own roommate.

Network map exercise (p. 68): A critical examination of the links in your network can make it more resilient to infiltration attempts.

4.14. Informants

Used in tactics: **Incrimination (p. 17)**

An informant (or *snitch*) is someone from inside a network recruited by an adversary to provide information on the network.

There are several different recruitment strategies: targeting people on the periphery of a network who are less committed, people who may face deportation if they don't cooperate, people who have been charged with another crime and are offered leniency or immunity in exchange, people who are no longer in a network and harbor feelings of resentment, people who prioritize money over dignity, etc. Informants are useful for **network mapping (p. 42)**.

Informants recruited by the State are often referred to as “confidential sources” in court proceedings.

See the informants topic[57].

Mitigations

Attack (p. 57): You can attack informants when uncovered or years later to discourage others from cooperating.

Background checks (p. 58): Background checks can help ensure that someone in your network is not an informant.

Need-to-know principle (p. 68): The need-to-know principle controls the flow of information through networks to make them more opaque and difficult to disrupt. If an informant isn't involved in an action, they shouldn't know who was involved even if it's their own roommate.

Network map exercise (p. 68): A critical examination of the links in your network can be a safeguard against placing your trust in people who could become informants.

Prisoner support (p. 71): Beyond the ethical imperative to support our prisoners, people are less likely to turn informant if they feel supported and connected to the movements for which they risked their freedom.

Repressive operations

Case against Marius Mason (p. 84): The main evidence against Marius Mason was provided to investigators by his former husband, Frank Ambrose, who had participated in some of the actions with him[59]. Frank Ambrose became an informant after his arrest in 2007 (which was

[58] https://actforfree.noblogs.org/post/2022/03/12/hamburgermany-incendiary-attack-on-the-car-of-former-police-spy-astrid-oppermann

[59] https://supportmariusmason.org/about-marius/about-the-case

triggered by him throwing incriminating material in a garbage can)[60]. For several months, the snitch collaborated extensively with the Federal Bureau of Investigation (FBI), secretly recording 178 phone conversations and face-to-face meetings, and providing information on 15 people[61].

4.15. International cooperation

Used in tactics: **Arrest (p. 18), Incrimination (p. 17)**

Several international organizations (such as Interpol) exist to facilitate the exchange of information across borders and the arrest and deportation of fugitives. Intelligence and police agencies from different countries routinely help each other by exchanging information, especially in high-profile cases.

Repressive operations

Bialystok (p. 79): In June 2020, comrades were arrested in Spain and France, thanks to cooperation between Italian, Spanish and French intelligence and police forces[62].

According to the investigation files, during the investigation Italian cops tried to target a person living in Germany[63]. They sent several requests to German police to extradite the person or have their house searched but the requests were rejected.

Scintilla (p. 81): Carla was arrested in France thanks to cooperation between Italian and French intelligence and police forces[44].

4.16. Interrogation techniques

Used in tactics: **Incrimination (p. 17)**

When interrogating suspects, an adversary can use a variety of interrogation techniques to get information from them. These may include lying, making threats, instilling guilt, shame, or pride, trying to appear friendly and helpful or, on the contrary, threatening and violent, etc.

For a comprehensive overview of interrogation techniques and how to resist them, see How the police interrogate and how to defend against it[64] (in French and German).

Mitigations

Avoiding self-incrimination (p. 57): You should not talk to an adversary under any circumstances: this is the best way to resist their interrogation techniques.

Repressive operations

Case against Boris (p. 77): When interrogating people close to Boris, investigators used elaborate lies to try to get information from them[18]. For example, the investigators vaguely suspected that the people being interrogated had hosted Boris in April 2020 and wanted to confirm their suspicion, so they asked, “Our investigation revealed that you let [Boris] stay with you in April 2020. How long did he stay with you?”

[60] https://www.mlive.com/news/ann-arbor/2008/10/activist_turned_informant_sent.html

[61] https://animalliberationpressoffice.org/NAALPO/snitches

[62] https://malacoda.noblogs.org/anarchici-imprigionati

[63] https://attaque.noblogs.org/post/2022/02/20/italie-allemagne-de-rome-a-bialystok-en-passant-par-berlin

[64] https://notrace.how/resources/#comment-la-police-interroge-et-comment-sen-defendre

4.17. Mass surveillance

Used in tactics: **Deterrence (p. 17)**, **Incrimination (p. 17)**

Mass surveillance includes any surveillance that can be a threat to anarchists and other rebels but does not have a specific target—the surveillance baseline of our society.

4.17.1. Civilian snitches

A civilian who witnesses a crime and identifies with the State is likely to call the police, provide a description of the suspect(s), and may even follow them until the police intervene or become a witness in a criminal investigation.

Mitigations

Anonymous dress (p. 54): By dressing anonymously, you can prevent civilians from providing a description of you that would be valuable to an adversary.

Attack (p. 57): If a citizen follows you after an action, you can scare them off with threats or pepper spray. If a citizen tries to call the police, you can destroy their phone.

Careful action planning (p. 60): Acting at night or in areas with minimal foot traffic minimizes witnesses, and a lookout can report the presence of any witnesses as soon as they are noticed. Beware of balconies and windows overlooking the scene.

Repressive operations

Belarusian anarcho-partisans (p. 77): While trying to cross the Belarusian-Ukrainian border, the anarchists stopped at a shop about 10 kilometers from the border. A shopkeeper called the border guards on them, which led directly to their arrest.

2019-2020 case against Mónica and Francesco (p. 78): The saleswoman of the cell phone store where Mónica bought a phone that was used as part of the 2020 action, when questioned by the police, gave a description of a person that the investigators matched to Mónica[38].

4.17.2. Mass digital surveillance

The Internet and digitization have reached many areas of life: financial transactions, biometric screening at borders, GPS tracking of smartphones, and "smart" streetlights. Combined with technological advances in storage capacity and processing power, this enables mass digital surveillance—the routine collection and analysis of vast amounts of data on everyone and everything for the needs of power.

See the digital surveillance topic[65].

Mitigations

Avoiding self-incrimination (p. 57): You should not store self-incriminating information on digital devices except for very deliberate reasons, such as writing and sending an action claim, and always through **Tails (p. 63)**.

Digital best practices (p. 63): Tor[66] renders mass digital surveillance ineffective by anonymizing Internet use. If Tor is not an option, using a VPN also increases your privacy by routing your Internet traffic through privacy-oriented services instead of your Internet Service Provider.

[65] https://notrace.how/resources/#topic=digital-surveillance

[66] https://torproject.org

Open-source and security-oriented operating systems and applications limit the data they store or collect about you as much as possible.

Encryption (p. 65): Encrypting “in motion” data renders the data unintelligible to observers at certain points on the network, such as State network monitoring centers.

4.17.3. Police files

Police files record a vast amount of data about many things, are kept indefinitely or for long periods of time, and can be efficiently analyzed and cross-referenced using digital tools.

Noteworthy examples of police files include:

- Databases of government-issued ID documents (ID cards, driving licenses, passports).
- Databases of biometric information (face photographs, fingerprints, DNA).
- Records of **ID checks (p. 35)**, fines, arrests, investigation proceedings, judicial proceedings, and convictions.

Mitigations

Attack (p. 57): You can destroy cabinets that store police files on paper and data centers that store them digitally.

Repressive operations

Case against Boris (p. 77): Investigators found out that the DNA on the bottle cap belonged to Boris because his DNA was in France's national DNA database[18].

Investigators obtained and analyzed records of local police activity (ID checks and fines) shortly before and after the sabotages, in different perimeters around where the sabotages took place, presumably hoping to find the names of the saboteurs in those records.

4.17.4. Video surveillance

Some countries now have more surveillance cameras than citizens. Video surveillance aims to capture the identity of everyone who passes through a space and to extend its coverage to as much space as possible for deterrence and incrimination.

If a crime occurs, relevant video footage can be analyzed retroactively; can the perpetrator be identified by their **face (p. 30)**, **gait (p. 31)**, physical characteristics, voice, etc.? Was there any suspicious activity in the time leading up to the crime? Surveillance cameras integrated into a central CCTV network can be monitored by humans in real time, either as part of routine police surveillance or during exceptional events (e.g. demonstrations).

Surveillance cameras can vary widely in quality, range, night vision capabilities, presence of microphones, etc. Video footage is increasingly processed by automated license plate readers or **facial recognition algorithms (p. 30)** to alert authorities to suspicious behavior or simply to automate the tracking of all individuals throughout their daily lives to facilitate the retrieval of something of interest.

In addition to traditional CCTV cameras, police can retrieve or request video footage from a variety of additional sources during an investigation:

- Cameras that monitor the exterior or interior of shops, offices, etc.
- Public transport cameras on buses, trains, highways, etc.
- Home surveillance systems such as Amazon Ring
- In-vehicle surveillance systems like those found on Teslas

See the topics video surveillance[67] and automated license plate readers[68].

Mitigations

Anonymous dress (p. 54): By dressing anonymously, you can prevent an adversary from identifying you from CCTV footage.

Anonymous purchases (p. 55): By taking steps to purchase items anonymously, video surveillance from stores should not be able to link you to materials used in an action.

Attack (p. 57): There are many ways[69] to disable surveillance cameras.

Biometric concealment (p. 59): When filmed by surveillance cameras:

- To prevent **gait recognition (p. 31)**, you can conceal your gait by wearing baggy clothes that hide your body shape, using an umbrella or other concealing objects, or drastically changing your walking style by adopting a "funny walk".
- To prevent **facial recognition (p. 30)**, you can wear a mask to cover your facial features, and sunglasses or a hat with a low brim to cover your eyes.

Outdoor and device-free conversations (p. 69): To avoid being picked up by surveillance cameras equipped with microphones, sensitive conversations should be conducted away from surveillance cameras.

Reconnaissance (p. 72): Before an action, you can identify the location of surveillance cameras and make plans to avoid them if possible.

Transportation by bike (p. 75): A bike is much harder to identify than other vehicles on CCTV footage, especially if its distinguishing features are minimized. You can use a different stolen bike for each action.

Repressive operations

Case against Boris (p. 77): Soon after the April sabotage, investigators requested CCTV footage from businesses and municipal cameras, and lists of vehicles from automated license plate readers (ALPRs) and speed cameras, all within an extended perimeter of the sabotage site[18].

Repression of Lafarge factory sabotage (p. 76): Immediately after the action, investigators requested CCTV footage from public transportation (buses, train stations, etc.), businesses, home surveillance systems, and municipal cameras, all within an extended perimeter of the action site[31]. In particular, footage of the interiors of buses appears to have helped identify people traveling to and from the action site[30]. Investigators also requested footage from highway toll booths, presumably to identify the occupants of known cars traveling on highways to or from the action site.

Prometeo (p. 80): According to the investigation files, two of the accused comrades were seen on a video surveillance camera leaving a store where investigators believe the envelopes used to prepare the parcel bombs were purchased[70].

Repression of the first Jane's Revenge arson (p. 76): CCTV footage helped identify a vehicle driven by the comrade who was later arrested, when they were seen entering a parking lot on foot after a demonstration, and the vehicle was seen leaving the same parking lot a few minutes later[34].

The three from the park bench (p. 79): On the evening leading up to the arrests, one of the comrades—while being followed by cops—stopped at a gas station and was seen by the station's

[67] https://notrace.how/resources/#topic=video-surveillance

[68] https://notrace.how/resources/#topic=automated-license-plate-readers

[69] https://notrace.how/resources/#detruisons-les-cameras

[70] https://ilrovescio.info/2020/08/23/uno-scritto-di-natascia-dal-carcere-di-piacenza

video surveillance cameras buying gas and filling a gas can[71]. The cops got the CCTV footage the next morning.

2019-2020 case against Mónica and Francesco (p. 78): Public CCTV footage was extensively used by investigators to reconstruct the movements of Mónica and Francesco before and during the attacks, despite the mitigations they took (taking taxis, changing clothes, wearing disguises)[38].

4.18. Network mapping

Used in tactics: **Incrimination (p. 17)**

Network mapping is the activity of gaining insight into the organization and social connections of a given network. It allows individuals to be singled out for extra scrutiny, arrest, or recruitment as **informants (p. 37)**.

The State very frequently uses social media friends lists (a form of **open-source intelligence (p. 43)**) for network mapping because they do not require a warrant or legal authorization.

Mitigations

Anonymous phones (p. 55): Anonymous phones, since they are not tied to their owners' identities, can limit the ability of an adversary to achieve network mapping.

Avoiding self-incrimination (p. 57): Self-incrimination not only endangers the individual, but also the rest of their network. If possible, refusing to provide an adversary with your identity, photographs, fingerprints, or DNA samples can limit their ability to perform network mapping.

Compartmentalization (p. 61): By compartmentalizing your different identities (or projects), you can limit the ability of an adversary to achieve network mapping.

Digital best practices (p. 63): Social networks can be obscured by limiting digital communications to end-to-end encrypted messaging on encrypted devices.

Fake ID (p. 66): Using a fake ID in the event of an ID check can protect against network mapping.

Need-to-know principle (p. 68): Gossip that could be used for network mapping should be avoided.

Network map exercise (p. 68): As long as they avoid being routed out of networks, infiltrators and informants end up building credentials through association, building intensive social profiles of everyone in the network, finding pressure points to instigate interpersonal and political conflict, entrapping people, and monitoring our daily lives, ultimately helping an adversary achieve network mapping. A critical examination of the links in your network, by protecting against infiltrators and informants, can protect against network mapping.

Repressive operations

Mauvaises intentions (p. 82): To prove that the accused comrades knew each other and were therefore likely accomplices, the investigators used several clues[33]:

- They were arrested at the same demonstrations
- They called each other on the phone regularly
- They lived in the same place for long periods of time, as shown by their phone records

[71] https://notrace.how/resources/#observationen-und-andere-argernisse

4.19. Open-source intelligence

Used in tactics: **Incrimination (p. 17)**

Open-source intelligence is the collection and analysis of data from open sources (social media platforms, news media, blogs, forums, public records…) to support an investigation.

Mitigations

Avoiding self-incrimination (p. 57): An adversary's ability to use open-source intelligence in investigations against you or your networks is limited if you don't use social media and generally avoid making any information about yourself or your networks public.

Repressive operations

Repression of Lafarge factory sabotage (p. 76): From the beginning of the investigation, police officers analyzed photos of the action posted on a website that contained metadata, including the name and serial number of a camera[31]. They asked the manufacturer to disclose the name of the buyer. The manufacturer provided the name of the store where the camera was sold. Within days, the combination of these two pieces of information made it possible to identify a person accused of taking the photos.

2019-2020 case against Mónica and Francesco (p. 78): The photos used to identify Mónica and Francesco in public CCTV footage were found on social media[38].

4.20. Parallel construction

Used in tactics: **Incrimination (p. 17)**

The State does not limit itself to lawful means in its investigations. Parallel construction is a law enforcement process of building a parallel, or separate, evidentiary basis for an investigation in order to conceal how an investigation was actually conducted.

For example, an intelligence agency collected incriminating digital evidence from a phone without a warrant, so a house raid is conducted to obtain the phone, where this evidence can then be "discovered", so that it is not thrown out at trial because it was obtained illegally.

A particular form of parallel construction is evidence laundering, in which one police officer illegally collects evidence and then "washes" it by passing it to a second officer who develops it and turns it over to prosecutors.

4.21. Physical surveillance

Used in tactics: **Incrimination (p. 17)**

Physical surveillance is the direct observation of people or activities for the purpose of gathering information. Physical surveillance is usually conducted by specially trained personnel called *surveillance operators*, organized into a *surveillance team*. A physical surveillance operation is called a *surveillance effort*. Because it requires the deployment of surveillance operators on the ground, sometimes for extended periods of time, physical surveillance is usually a resource-intensive and personnel-intensive method of surveillance.

4.21.1. Aerial

Aerial physical surveillance is the direct observation of people or activities from the air for the purpose of gathering information. In many countries, helicopters have traditionally been the predominant tool for this purpose. As drones become less expensive, their use is becoming more common. Surveillance planes are also occasionally used and are much more covert than helicopters.

Examples of aerial physical surveillance include:

- Observing crowds during demonstrations or gatherings, often as part of an **overt (p. 46)** surveillance effort.
- Improving the chances of successfully following the target of surveillance during a **mobile physical surveillance (p. 45)** operation, especially at night.
- Locating suspects soon after an action took place and the adversary has been alerted, especially in rural areas or at night (in the case of an arson in Germany, a police helicopter responded by flying over the area the same night[72]).
- Locating suspects as part of routine **police patrols (p. 47)** in areas at risk of criminal activity.

Surveillance planes can monitor entire cities, photographing up to 32 square miles per second, allowing for the slow-motion reconstruction of virtually any outdoor movement[73], with high-quality video at night[74].

See the aerial surveillance topic[75].

Mitigations

Anonymous dress (p. 54): If you are being followed by an aerial surveillance effort, you can change into anonymous clothing when you are in a location that is not visible from the air to help prevent the aerial surveillance effort from re-establishing contact with you when you emerge into an open area (this won't work if the surveillance effort is also observing you on the ground).

Anti-surveillance (p. 56): You can include in an anti-surveillance route locations that cut off visibility from above—an underground metro system, a shopping complex with many entrances, etc.

Attack (p. 57): During demonstrations, you can take down drones with fireworks, hack them, or blind them with lasers. See also 5 widely accessible ways to take down drones[76].

Surveillance detection (p. 73): You should be able to see and hear most helicopters and some drones, depending on their altitude and your surroundings.

Repressive operations

Berlin 2023 railway conspiracy case (p. 76): The arrested comrades were discovered at night by a helicopter on a routine surveillance flight, presumably equipped with night-vision equipment[77]. A text[78] reports that in 2022, during another routine surveillance flight near Berlin, the same helicopter turned off its position lights and muffled the sound of its rotor blades to avoid detection: "Although the helicopter could still be heard, the noise was diminished. This can lead to

[72] https://actforfree.noblogs.org/post/2023/11/13/munich-germany-geothermal-energy-gets-hot-and-not-only

[73] https://theintercept.com/2020/04/09/baltimore-police-aerial-surveillance

[74] https://theintercept.com/document/2021/08/31/motion-to-suppress-aerial-surveillance-evidence-in-u-s-vs-muhammed-momtaz-alazhari

[75] https://notrace.how/resources/#topic=aerial-surveillance

[76] https://notrace.how/resources/#cinq-manieres-a-la-portee-de-tous-pour-abattre-un-drone

[77] https://notrace.how/resources/#wir-haben-eine-verabredung

[78] https://kontrapolis.info/9821

misjudging the distance of the helicopter or, if mixed with other noise such as a highway, not being aware of the approaching problem until it's too late.".

Repression of the 2019 uprising in Chile (p. 78): Drones were used to track rioters leaving the riot in order to facilitate their arrest[24].

4.21.2. Mobile

Mobile physical surveillance is the direct observation of a moving target for the purpose of gathering information. It is typically conducted by a surveillance team of five to twenty operators using multiple vehicles. During a mobile physical surveillance effort, the surveillance team has two goals: to successfully follow the target and to avoid being detected by the target.

A mobile physical surveillance effort typically begins with staking out the location where the target is believed to be, such as their home or place of employment. When the target leaves the stakeout location, the surveillance team begins following them and the surveillance effort transitions into a mobile phase. The surveillance effort then alternates between static phases (when the target stops) and mobile phases (when the target starts moving again).

Examples of mobile physical surveillance techniques include:

- Using an appropriate mode of travel based on the target's mode of travel. For example, if the target is in a vehicle, the surveillance team must use vehicles, but if the target is on foot, the surveillance team may prefer to use operators on foot.
- Using cover and concealment to avoid detection by the target. For example, surveillance vehicles can hide behind other vehicles, and surveillance operators on foot can blend in with pedestrian traffic.
- Rotating which surveillance operator or vehicle is closest to the target to limit the risk of the target noticing that someone is following them.

Mobile physical surveillance may be facilitated by:

- A **tracking device (p. 21)** installed on the target's vehicle or bike.
- **Aerial surveillance (p. 44)**, such as a drone following the target from a distance.

In rare cases, a mobile physical surveillance effort may lead to the arrest of the target if enough information has been gathered about the target's activities to incriminate them and immediate arrest is deemed necessary (e.g. to prevent a crime).

See also:

- Measures Against Surveillance[79] for insights into how police and intelligence agencies conduct such surveillance and how we can defend against it.
- The physical surveillance topic[80].

Mitigations

Anti-surveillance (p. 56): You can use anti-surveillance to evade a mobile physical surveillance effort.

Surveillance detection (p. 73): You can use surveillance detection to detect a mobile physical surveillance effort.

Transportation by bike (p. 75): It is more difficult for a mobile physical surveillance effort to follow a bike than other vehicles or someone on foot, especially without being detected.

[79] https://notrace.how/resources/#massnahmen-gegen-observation

[80] https://notrace.how/resources/#topic=physical-surveillance

Repressive operations

Case against Boris (p. 77): For several weeks, investigators regularly staked out Boris's home and tailed him as he moved on foot, on bicycles, and in vehicles[18].

Repression of the first Jane's Revenge arson (p. 76): In March 2023, cops secretely observed the comrade who was later arrested from a distance of about 30 meters[34]. The cops watched the comrade discard a paper bag, retrieved it, and collected DNA evidence linking the comrade to the crime scene.

Case against Jeff Luers (p. 83): On the night of the June arson, the arsonists were being tailed by a surveillance team—police officers in one or more unmarked cars—as they drove to the arson site[49]. They parked their car close to the arson site, watched by the surveillance team. They got out of their car to continue on foot, at which point the surveillance team lost sight of them. They ran back to their car 10 minutes later, at which point the surveillance team regained sight of them. They drove away from the arson site. More than an hour later, the surveillance team—still tailing the arsonists—heard on the police radio system about a fire at the arson site and asked local police officers to stop the arsonists' car, suspecting that they were involved in the fire. Half an hour later, when fire investigators at the arson site reported that they believed the fire had been set intentionally, the arsonists were arrested.

The three from the park bench (p. 79): During the evening leading up to the arrests, two of the comrades rode their bikes through the city and were followed by cops on bikes (and presumably also cops in cars) until they were arrested in the park[71]. The cops decided to follow the comrades specifically that evening because it was exactly two years since the G20 summit in Hamburg and the comrades were suspected of planning an action for the anniversary of the summit. The surveillance of one of the accused had started in March 2018[71].

Nea Filadelphia case (p. 82): On the day of the arrests, when one of the comrades visited a cybercafé that was probably under police surveillance, the cops recognized him and started following him[81]. He then moved through the streets of Athens for a few hours, gradually joining the other comrades—some of whom were wanted by the cops[82]—and all of them were arrested.

4.21.3. Overt

Overt physical surveillance is the direct observation of people or activities when the surveillance operators intend to be, or do not mind being, detected by their targets. This is common practice at demonstrations and gatherings to identify participants, whether to facilitate **network mapping (p. 42)** or to incriminate individuals for actions carried out during the demonstration.

Overt physical surveillance of just a few individuals is rare, and is often intended more to deter illegal activity by creating paranoia than to incriminate.

Mitigations

Anonymous dress (p. 54): By dressing anonymously at a demonstration or other event, you can prevent overt surveillance efforts from identifying you.

Repressive operations

Mauvaises intentions (p. 82): During a demonstration, the investigators took 180 photographs from which they obtained 200 portraits of the demonstrators, including ten people they were able to identify[33].

[81] https://web.archive.org/web/20201027031238/http://actforfree.nostate.net/?p=15472

[82] https://machorka.espivblogs.net/2013/11/06/letter-from-anarchists-argiris-dalios-and-fivos-harisis-from-koridallos-prisons-athens

4.22. Police patrols

Used in tactics: **Arrest (p. 18)**, **Deterrence (p. 17)**, **Incrimination (p. 17)**

Police patrol areas in vehicles or on foot, either as routine patrols or in response to a perceived threat in a particular area. In some contexts, unmarked vehicles are used for patrols.

Routine patrols usually occur in extended perimeters around police stations. They serve to establish a visible presence that can have a deterrent effect, and occasionally to catch unlucky criminals "red handed". Except maybe in remote areas, routine patrols can always happen and should be taken into account when planning an action.

If the police are made aware of a threat in a particular area which they consider to be worthy of investigation, they will send one or more patrols to investigate it. The time between when they are made aware of the threat and the arrival of the patrols depends on the distance between the area to investigate and the nearest available police unit. The police can be made aware of a threat by:

- A routine patrol stumbling upon a crime by chance.
- **Guards (p. 33)** or **civilians (p. 39)**.
- An **alarm system (p. 19)** (e.g. motion detectors inside a building), either directly or through a security company monitoring the alarm system.
- Police officers monitoring live footage in **CCTV centers (p. 40)**.
- An **infiltrator (p. 36)** or an **informant (p. 37)**.

Mitigations

Attack (p. 57): To reduce the likelihood of a police patrol disturbing an action, you can distract the police by launching a near-simultaneous attack on the other side of the neighborhood, or disrupt their communications by burning the cell tower used for police communications. To prevent a police patrol from following you after an action, or to slow them down, you can use some tactics either preventively or during the pursuit: crow's feet or spike strips, gunfire, barricades, stones, fireworks, etc.

Reconnaissance (p. 72): Before an action, you can identify the nearest police station, their shift change schedule, and patrol patterns. You can identify routes that are not visible to police patrols and that would make pursuit difficult (forests, railroad tracks, etc.).

4.23. Service provider collaboration

Used in tactics: **Incrimination (p. 17)**

Service providers that hold information about you can be asked or legally compelled to provide this information to the police, both retrospectively and in real time.

Noteworthy examples of service providers, along with the information they can provide, include:

- Websites, email providers, and other online services: the content of unencrypted communications (e.g. social media posts, unencrypted email) and metadata about encrypted communications (e.g. the sender, recipient and date of encrypted email).
- Internet service providers:
  - If you follow **digital best practices (p. 63)** and use Tor: metadata about your Internet activity, such as when you use Internet.
  - If you don't use Tor: your Internet activity, including the list of websites you visit.

- Mobile network operators: the content of SMS and regular calls, the list of websites you visit, your phone physical location, metadata about your use of encrypted messaging applications (e.g. when you use Signal and the approximate size of messages sent or received through Signal).
- Banks:
  - Bank account activity, including the date, location and amount of any purchase or withdrawal made with a card.
  - Video surveillance footage from cameras on ATMs.
- Social services, hospitals, and other State institutions: any information they hold about you, including your address, marital status, social benefits, health information, etc.

Mitigations

Anonymous phones (p. 55): If you use an anonymous phone, an adversary cannot easily use the collaboration of mobile network operators to establish a link between your identity and the phone number. This means that:

- If they know your identity, they won't be able to learn the phone number and tap its communications.
- If they know the phone number, they won't be able to learn your identity.

Still, there is a way for the adversary to link your identity to an anonymous phone number using cell tower data provided by mobile network operators. If the adversary knows that you were in place A on Monday and in place B on Tuesday, and they know from cell tower data that a particular phone was the only phone that was also in place A on Monday and in place B on Tuesday, the phone is probably yours.

Digital best practices (p. 63): Using a trusted service provider[83] means that they will refuse to comply with an adversary's requests to access your data, or build their service to make it technically impossible to comply with such requests. Using peer-to-peer applications such as Cwtch[84] and Briar[85] for communication or OnionShare[86] for file sharing avoids the need to trust a service provider.

Encryption (p. 65): Encrypting "in motion" data limits the ability of untrusted service providers to collaborate with an adversary. For example, your Internet Service Provider will be able to collect much less data about your Internet activity if you use Tor[66] or a Virtual Private Network (VPN).

Repressive operations

Case against Boris (p. 77): With the collaboration of mobile network operators, investigators intercepted calls from Boris's phone or the phones of people close to him[18]. They regularly listened to the intercepted calls in real time and used information from the calls to adjust ongoing **physical surveillance (p. 43)** operations.

With the collaboration of the email provider, investigators gained real time access to an email address used by Boris: they were able to see emails sent and received in real time.

Repression against Zündlumpen (p. 78): One clue against a suspected editor of the newspaper is that she used her bank account to order things that could be used for printing—her bank records were presumably obtained by the police with the collaboration of the bank[28].

[83] https://riseup.net/en/security/resources/radical-servers

[84] https://cwtch.im

[85] https://briarproject.org

[86] https://onionshare.org

Prometeo (p. 80): Investigators distorted conversations obtained through phone interception to make them look suspicious[70]. During a phone conversation involving one of the accused comrades, the phrase "tutta questa tensione sociale prima o poi scoppierà" ("all this social tension will, sooner or later, explode") was said, which was only partially transcribed in the investigation files as "prima o poi scoppierà" ("will, sooner or later, explode").

Mauvaises intentions (p. 82): The collaboration of mobile network operators was used to link phone numbers to civil identities, to know which phone numbers were in contact with each other, to geolocate phones (both retrospectively and in real time) and to record phone calls[33].

4.24. Targeted digital surveillance

Used in tactics: **Incrimination (p. 17)**

Targeted digital surveillance is used to compromise the use of digital devices.

Extremely advanced techniques also exist[87] in the arsenal of nation-state actors, although the focus here is on techniques that are more likely to be used.

See the digital surveillance topic[65].

4.24.1. Authentication bypass

Full Disk Encryption (p. 65) is used to protect access to a device—it is what is unlocked during authentication when you enter your password upon booting a device. This authentication can be bypassed either through human error, weak passwords, or technical exploits.

Ways to bypass authentication to an encrypted device include:

- Accessing the device while it's powered on
- Finding the password written down somewhere
- Pressuring the device owner into providing the password by using legal threats or, in some contexts, **extra-legal violence (p. 25)**
- Visual interception: watching the device owner type the password through a **hidden camera (p. 23)** or an **infiltrator (p. 36)**
- Brute force: guessing the password through repeated, automated authentication attempts
- Compromising the device either through **malware (p. 51)** or **physical access (p. 53)**
- Exploiting a flaw at the implementation level of the encryption process

Companies such as Cellebrite and Graykey contract their technology to attack authentication on mobile devices, either through exploits or brute force password guessing.

Mitigations

Bug search (p. 59): Before entering a password in a room where a **hidden camera (p. 23)** may be present, you can search the room using appropriate techniques and tools to locate and possibly remove such a camera.

Since it's not possible to be certain that a camera is not present, you can enter the password while under an opaque sheet or blanket.

Digital best practices (p. 63): Using secure operating systems with Full Disk Encryption (FDE) and strong passwords should prevent authentication bypass. For example, on phones GrapheneOS implements encryption[88] to make brute-force password guessing impossible—after 140

[87] https://anonymousplanet.org/guide.html#some-advanced-targeted-techniques

[88] https://grapheneos.org/faq#encryption

failed attempts, each is delayed for a full day. On computers, the forensics department of the German federal police was unable to decrypt Linux FDE (called LUKS), used by many Linux systems such as Debian[89] and Tails[39], after a year of effort[90]. FDE on MacOS, Windows, iPhone or stock Android should not be relied upon.

Tamper-evident preparation (p. 74): You can detect when a device has been **physically accessed (p. 53)** with tamper-evident preparation.

Once a device has been physically accessed by an adversary, you should consider it compromised and never authenticate to it again. This is because, in a worst-case scenario, the adversary may have copied the device's data and compromised its firmware so that when you enter your password, they can remotely obtain it and use it to decrypt the data.

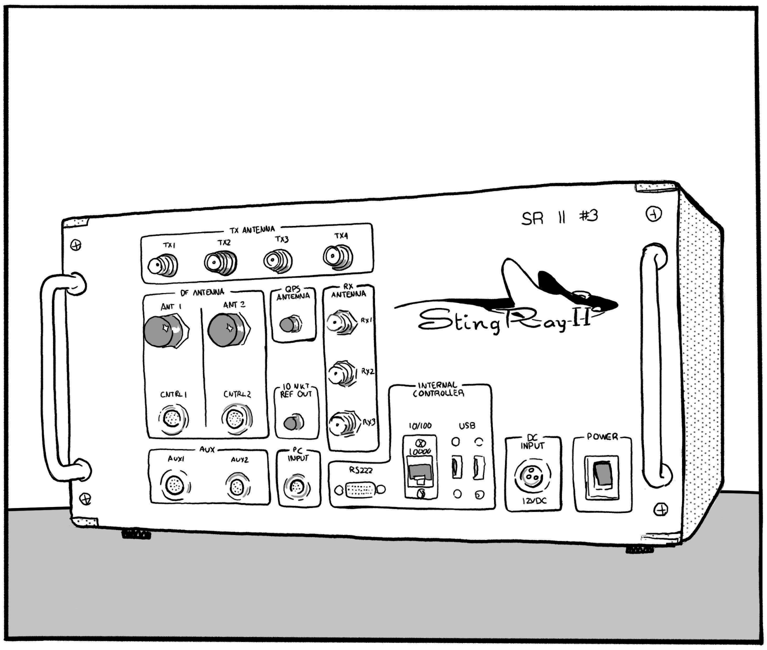
Repressive operations

Repression against Zündlumpen (p. 78): In some of the April 2022 raids, cops seized smartphones immediately after entering and plugged them into power banks, presumably to prevent them from shutting down and reverting to an encrypted state[91].

Repression of Lafarge factory sabotage (p. 76): Investigators recovered several encrypted smartphones in the raids and attempted to access their encrypted data, with varying results depending on the phone[31]:

- For the iPhones that were recovered turned on, they exploited the security vulnerabilities that exist when they are turned on to bypass their encryption and access the encrypted data.
- For all Android phones (whether recovered on or off) and one iPhone recovered off, they extracted the phones' encrypted partitions and attempted to brute force them from a computer.

4.24.2. IMSI-catcher



[89] https://debian.org

[90] https://notrace.how/resources/#observationen-und-andere-argernisse

[91] https://zuendlappen.noblogs.org/post/2022/05/07/muenchen-ueber-razzien-und-ein-%c2%a7129-verfahren-gegen-anarchistinnen-und-den-raub-einer-druckerei

An IMSI-catcher (also known as a Stingray) is an eavesdropping device used to obtain information about all mobile phones that are turned on in a limited area around the device. The information that can be obtained about a phone includes its number, its unique International Mobile Subscriber Identity (IMSI) number, and all cellular traffic (texts, calls, and Internet traffic). A passive IMSI-catcher simply listens to the traffic, while an active IMSI-catcher acts as a "fake" cell tower between the phones and the service provider's real towers.

IMSI-catchers are often used to link people and phone numbers, for example:

- At a public demonstration, to record the phone numbers of all phones present at the location and later obtain the names associated with those phone numbers from mobile network operators.
- As part of a **physical surveillance (p. 43)** operation: If an adversary is following you, they can use an IMSI-catcher to find your phone number or the phone numbers of people you are meeting with.

They can also be used to actually intercept traffic, for example:

- To intercept the traffic of a target cell phone without having to get the **cooperation of the mobile network operator (p. 47)** through a warrant.
- To intercept traffic from a target mobile phone when the adversary knows where it's being used, but doesn't know the phone number.

See the IMSI-catchers topic[92].

Mitigations

Bug search (p. 59): With the proper techniques and tools, or simple visual observation, you can detect the presence of an IMSI-catcher. Such a detection can have various benefits:

- The simple presence of an IMSI-catcher is a valuable clue as to the level of surveillance employed by an adversary.
- If the IMSI-catcher is used during an event or demonstration, you can persuade all participants to turn off their phones.
- You can destroy the IMSI-catcher (professional IMSI-catchers can be very expensive).

Encryption (p. 65): If a phone's "in motion" data is encrypted, it is unintelligible to an IMSI-catcher. For example, you should use end-to-end encrypted messaging applications instead of legacy texts and calls for your phone communications.

Repressive operations

Case against Boris (p. 77): Investigators used IMSI-catchers during **physical surveillance (p. 43)** operations to find the phone numbers of people Boris was meeting with—and then identified those people by asking mobile network operators for the names corresponding to the phone numbers[18].

4.24.3. Malware

Malware is malicious software that compromises a computer, server, or mobile phone. What this malicious software does is highly context-dependent, but against anarchists and other rebels it typically involves gaining visibility into the device through remote screen capture and remote keylogging (recording the keys pressed on a keyboard), as well as location tracking in the case of phones.

[92] https://notrace.how/resources/#topic=imsi-catchers

The vast majority of State malware installations occur through phishing, either via email or text-based messages (SMS, etc.). To be effective, phishing often requires the target to open a malicious file or link. Malware can also be installed through **physical access (p. 53)**, such as the insertion of a malicious USB device.

See the targeted malware topic[93].

Mitigations

Compartmentalization (p. 61): You can use different Tails[39] USB sticks or Qubes OS[94] virtual machines for different digital identities. This way, if an adversary compromises one stick or virtual machine with malware, the compromise won't spread to other sticks or virtual machines.

Computer and mobile forensics (p. 62): You can sometimes detect traces of malicious software on a device after the fact.

Digital best practices (p. 63): Using security-oriented operating systems and other digital best practices makes malware installation less likely. Phishing awareness is also important—don't open attachments or click on links sent to you by people you don't trust.

Encryption (p. 65): Encrypting "in motion" data can complicate network packet injection—an installation vector for some forms of modern spyware, such as Pegasus[95].

Repressive operations

Scripta Manent (p. 83): Malware was installed on the computer of one of the accused comrades[96]. According to the investigation files, the malware, which was installed remotely over the Internet, targeted a Windows computer and was capable of recording text typed on the keyboard, taking periodic screenshots, and recording communications sent and received to and from the computer.

Repression of Lafarge factory sabotage (p. 76): According to the case files, investigators made five requests to remotely install spyware[31]. Of these, one installation was successful (on an iPhone SE 2020) and provided access to a Signal group conversation.

4.24.4. Network forensics

Network forensics is the monitoring and analysis of network traffic.

Network information is volatile, it is designed to be transmitted and then lost, so monitoring it requires a proactive approach. Many countries have built network monitoring centers that store massive amounts of network information for days, months, or years to be analyzed later. An adversary can also monitor your network traffic with the **collaboration of your Internet Service Provider (p. 47)**, by compromising your home router with **malware (p. 51)**, or by snooping on your wired or wireless network connection from a surveillance vehicle outside your home.

Because most websites, email providers, and messaging applications use SSL/TLS encryption (the "s" in "https"), an adversary monitoring your network traffic usually knows what websites you visit, but not what you do on those websites. If you use Tor[66], an adversary monitoring your network traffic knows that you use Tor, but not what websites you visit or what you do on those websites.

Tor is vulnerable to correlation attacks, but such attacks are difficult to set up even for powerful adversaries. An example of a successful correlation attack can be found in the prosecution of

[93] https://notrace.how/resources/#topic=targeted-malware

[94] https://www.qubes-os.org

[95] https://forbiddenstories.org/about-the-pegasus-project

[96] https://earsandeyes.noblogs.org/post/2019/01/27/more-precisions-keylogger-italy

anarchist hacker Jeremy Hammond, in which the times when the alias he used in chat rooms was "online" (obtained through network traffic analysis[97]) were correlated with the times when a **physical surveillance (p. 43)** effort observed him at home to prove that the alias belonged to him.

Mitigations

Compartmentalization (p. 61): Different digital identities can be correlated through the footprints left by their network traffic. To limit this risk, you can compartmentalize different digital identities by using Tails[39] and rebooting between each session, or on Qubes OS[98] by using different Whonix[99] virtual machines non-simultaneously.

Digital best practices (p. 63): If you use Tor[66] or a VPN, it is harder for an adversary to analyze your network traffic.

Encryption (p. 65): If you encrypt your network traffic with Tor[66] or a VPN, it is harder for an adversary to analyze it.

4.24.5. Physical access

If an adversary has gained physical access to your electronic device at any point, you must assume that the device has been compromised. Physical access can be used to read unencrypted content or to manipulate the device digitally or physically (for example, to install spyware or a physical keylogger).

Physical access can be obtained during border customs inspections, after arrest if you have the device on you, during a **house raid (p. 34)** or **covert house search (p. 20)**, and by an **infiltrator (p. 36)** or **informant (p. 37)** you trust to use the device.

Mitigations

Computer and mobile forensics (p. 62): You can sometimes detect physical access to a device after the fact.

Digital best practices (p. 63): Don't take your phone with you if you're likely to be arrested, and ideally leave it at home as much as possible.

Network map exercise (p. 68): A critical examination of the links in your network can help you decide who to allow to use your devices based on established trust.

Physical intrusion detection (p. 70): You can detect physical access to a space with motion-activated cameras that send remote alerts when detected and tampered with.

Tamper-evident preparation (p. 74): Tamper-evident preparation makes it possible to detect when something has been physically accessed.

[97] https://medium.com/beyond-install-tor-signal/case-file-jeremy-hammond-514facc780b8

[98] https://qubes-os.org

[99] https://whonix.org

5. Mitigations

5.1. Anonymous dress

Techniques addressed by this mitigation:

Forensics > Facial recognition (p. 30)
Forensics > Gait recognition (p. 31)
Forensics > Trace evidence (p. 32)
Mass surveillance > Civilian snitches (p. 39)
Mass surveillance > Video surveillance (p. 40)
Physical surveillance > Aerial (p. 44)
Physical surveillance > Overt (p. 46)

Anonymous dress is the practice of wearing clothing with two goals in mind: to hide your body features, and to ensure that the clothing itself cannot be used to identify you.

To hide your body features, you can:

- To hide your face: wear a mask that adequately covers your face, including your eyebrows and up to the top of your nose.
- To hide the rest of your body: wear a shirt with long sleeves, gloves, pants with long legs, and high socks.
- To hide your skin color: make sure no skin is visible, including around your eyes, at the junction of your shirt and gloves, and at the junction of your pants and socks.
- To hide your body shape and gait: wear baggy clothing (you can also conceal your gait with **biometric concealment (p. 59)**).

To ensure that clothing used during an action cannot be used to identify you, you can:

1. **Anonymously purchase (p. 55)** two sets of clothing specifically for the action, "civilian clothing" and "action clothing":
    - Civilian clothing is clothing that is normal to wear in public. It can include items that hide your body features as long as it isn't suspicious (e.g., a hat, a "Covid" mask).
    - Action clothing is clothing that adequately hides your body features, as described above.
2. Far away from the action site, change from your regular clothing into the civilian clothing, in a suitable place where there are no surveillance cameras or witnesses.
3. Close to the action site, change into the action clothing (in a suitable place).
4. Perform the action.
5. Close to the action site, change back into the civilian clothing (in a suitable place).
6. Far away from the action site, change back into your regular clothing (in a suitable place).
7. Dispose of the civilian clothing and the action clothing safely.

A specific form of anonymous dress is the "black bloc" tactic, in which a large number of people at a demonstration all dress as similarly as possible, typically in black, so as to be indistinguishable from one another.

5.2. Anonymous phones

Techniques addressed by this mitigation:

Network mapping (p. 42)
Service provider collaboration (p. 47)

An anonymous phone is a phone that is not tied to your identity. For a phone to be anonymous, the device itself, its SIM card, and its plan must all be **purchased anonymously (p. 55)**. Because **mobile network operator collaboration (p. 47)** can reveal the history of a phone physical location, an anonymous phone should not be turned on close to where you live. A burner phone is a type of anonymous phone that is discarded shortly after use.

Anonymous phones can be used for sensitive projects or actions where the need for a phone was found to be unavoidable. Unless a phone number needs to be stable in the long term, burner phones should always be preferred.

Pseudo-anonymous phones that you have purchased anonymously but use where you live can mitigate **network mapping (p. 42)**—especially if all members of a scene or network use them—but should not be used for sensitive projects or actions.

See Burner Phone Best Practices[100] for more information on burner phones.

5.3. Anonymous purchases

Techniques addressed by this mitigation:

Forensics > Arson (p. 26)
Forensics > Ballistics (p. 26)
Mass surveillance > Video surveillance (p. 40)

Any materials meant to be used in a sensitive action or project should be purchased anonymously. The goal is to prevent materials found at an action site (e.g. an incendiary device with a delay that failed) or traces from such materials (e.g. accelerant traces discovered by **arson forensics (p. 26)**) to be linked back to you.

Anonymous purchases in physical stores should be made well in advance, with staggered times and locations to make it difficult to analyze CCTV footage, and should be considered a "protected activity" that is preceded by **anti-surveillance (p. 56)**. Payments should always be made in cash and the interaction with the cashier should not be memorable. Some level of **anonymous dress (p. 54)** can be used to be less recognizable on CCTV footage—a Covid mask, a hat, dedicated clothing.

Digital anonymous purchases are possible with cryptocurrencies. Unless the cryptocurrencies are acquired anonymously they must be sufficiently laundered before being used, which can be a hassle, but is possible with cryptocurrencies such as Monero using Tails[101].

See Prisma[102] for more details on anonymous purchases in physical stores.

[100] https://notrace.how/resources/#burner-phone-best-practices

[101] https://anonymousplanet.org/guide.html#your-cryptocurrencies-transactions

[102] https://notrace.how/resources/#prisma

5.4. Anti-surveillance

Techniques addressed by this mitigation:

Physical surveillance > Aerial (p. 44)
Physical surveillance > Mobile (p. 45)

Anti-surveillance is the practice of taking active measures to evade ("shake off") a **mobile physical surveillance effort (p. 45)**.

There are two, and only two, scenarios in which you should conduct anti-surveillance:

- **If you are on the move to conduct an activity that you don't want an adversary to observe, and you have no indication that you are being followed**, you can conduct anti-surveillance to evade a potential surveillance effort that could be following you. The goal of conducting anti-surveillance in this scenario is to minimize the risk of being followed when you conduct the planned activity.
- **If you have an indication that you are being followed, and you suspect that the surveillance effort is planning to take immediate violent action against you** (e.g., arrest or attack you), you can conduct anti-surveillance. The goal of conducting anti-surveillance in this scenario is to avoid the suspected violent action.

You should not conduct anti-surveillance in other scenarios because:

- If you are on the move to conduct an activity that you don't want an adversary to observe, but you have an indication that you are being followed, you would not be able to conclusively determine that the anti-surveillance measures you took successfully allowed you to evade the surveillance effort. Therefore, you would cancel the planned activity in any case, making anti-surveillance useless.
- If you have an indication that you are being followed, but you don't suspect that the surveillance effort is planning to take immediate violent action against you, conducting anti-surveillance would reveal to the surveillance effort that you know they are following you, which could push the adversary to adapt and be more discreet, which you want to avoid.

A core principle of anti-surveillance is that, usually, a surveillance effort really doesn't want to be detected by its target, and would rather lose its target than risk detection. Because of this, most anti-surveillance measures you take should:

- Attempt to provoke one of two situations: either the surveillance operators expose themselves in a way that you can detect, or they lose you.
- Be paired with **surveillance detection (p. 73)** so that you can detect operators who have exposed themselves because of the anti-surveillance measure.

Anti-surveillance is an advanced practice. Before conducting anti-surveillance, we recommend that you read up on it using the links at the end of this description. That said, examples of anti-surveillance include:

- Entering a "blind spot" of a surveillance effort, that is, a space where they lose sight of you, and then conducting a series of evasive maneuvers, all the while attempting to detect surveillance operators. For example, if you are on foot in a city, you can enter a crowded public building, quickly exit through a back door, and then conduct more evasive maneuvers. If you notice people rushing to enter the building after you, or looking for you on the street after you exit the building, they may be surveillance operators.
- Moving from an open area, where a surveillance effort needs to stay far away from you to avoid detection, to a less open area, where the surveillance effort needs to come closer to you to avoid losing you, all the while attempting to detect surveillance operators. For example, if

you are on a bike in a rural area, you can move from a road where you can see far ahead and behind you to a small forest path, then accelerate, go deep into the forest, and come out of the forest far from where you entered, in a place that a surveillance effort would not expect. If you notice people acting strangely as you enter or exit the forest, they may be surveillance operators.

If an adversary notices that you are conducting anti-surveillance, they may adapt and become more discreet. Therefore, when conducting anti-surveillance, you should avoid revealing that you are doing so, if possible.

See the physical surveillance topic[80].

5.5. Attack

Techniques addressed by this mitigation:

Alarm systems (p. 19)
Guards (p. 33)
Increased police presence (p. 35)
Infiltrators (p. 36)
Informants (p. 37)
Mass surveillance > Civilian snitches (p. 39)
Mass surveillance > Police files (p. 40)
Mass surveillance > Video surveillance (p. 40)
Physical surveillance > Aerial (p. 44)
Police patrols (p. 47)

Many repressive techniques are effectively mitigated by a simple maxim: the best defense is a strong offense.

Mass digital surveillance is impossible if the Internet backbone has been taken offline by cutting fiber optic cables. Video surveillance depends not only on network connectivity, but also on physical cameras that are too decentralized to effectively protect against sabotage. A witness can be intimidated into not testifying in an upcoming trial if the car outside their house is torched while they sleep. Informants and infiltrators can be immiserated and attacked in countless creative ways. Increased police presence somewhere means the possibility of decreased police presence somewhere else. Forensic labs can go up in smoke. Police communications depend on TETRA[103] and P25[104] antennas, and police operations depend on the integrity of their vehicle fleets, stations, and individual officers' feelings of safety. The possibilities for attack are limited only by one's imagination.

5.6. Avoiding self-incrimination

Techniques addressed by this mitigation:

Door knocks (p. 23)
Forensics > Digital (p. 29)
ID checks (p. 35)
Interrogation techniques (p. 38)
Mass surveillance > Mass digital surveillance (p. 39)

[103] https://en.wikipedia.org/wiki/Terrestrial_Trunked_Radio#Usage
[104] https://en.wikipedia.org/wiki/Project_25

Network mapping (p. 42)
Open-source intelligence (p. 43)

An enormous number of convictions are based on self-incrimination—behaviour that essentially amounts to snitching on yourself.

Don't talk to the adversary: in the event of arrest, any communication with the adversary beyond the legal requirements (often name, date of birth, and address) should be considered self-incrimination, and depending on your context there may be a precedent for being released without divulging even this information.

Don't brag about crimes to friends, comrades, or cellmates—even if you have a solid foundation of trust, the knowledge unnecessarily endangers the person you're telling and could be overheard by a surveillance effort.

Digital communications and devices are hostile terrain; if you don't want it read back to you in court, don't let it go through your phone as a text message, photo, etc.—regardless of **encryption (p. 65)**. Another treasure trove for the adversary is social media, and messages or posts are regularly used in prosecutions. Don't take videos or photos during riots—this incriminates your networks and should be considered a form of snitching[105].

Refusing to provide identification and biometric information (face photograph, fingerprints, DNA) upon arrest can be a viable strategy, but is highly context-dependent.

See the related mitigation **Need to know principle (p. 68)**.

5.7. Background checks

Techniques addressed by this mitigation:
Infiltrators (p. 36)
Informants (p. 37)

Background checks are used to verify that a person is who they claim to be. They can help ensure that someone in your network isn't an infiltrator, informant, or otherwise lying about their identity for malicious reasons.

Performing a background check on someone may involve:

- Contacting or meeting their friends or family to ask questions about them.
- Visiting their home or place of employment.
- Reviewing their identity or administrative documents (employment or rental history, criminal record, etc.)

We recommend two different approaches to background checks:

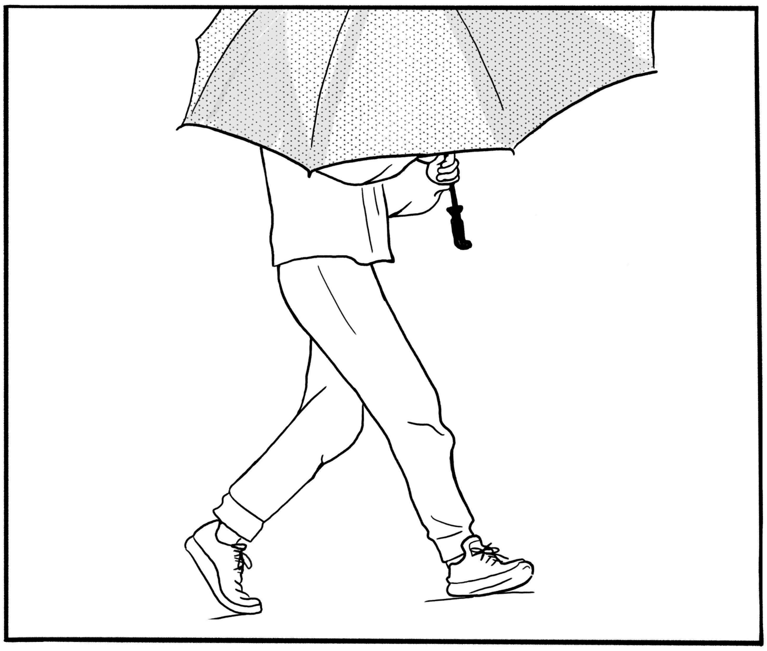
- The consensual, mutual approach: If you already trust someone to some degree but would like to trust them more, you can do a mutual background check, where each of you checks the other.
- The non-consensual approach: If you already have strong suspicions that someone is lying about their identity, you can do a background check on them without their consent to confirm your suspicions.

For more information on background checks, see Confidence, Courage, Connection, Trust[106].

[105] https://rosecitycounterinfo.noblogs.org/2022/08/uprising-lessons

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

5.8. Biometric concealment



Techniques addressed by this mitigation:

Forensics > Facial recognition (p. 30)
Forensics > Gait recognition (p. 31)
Forensics > Handwriting analysis (p. 31)
Forensics > Linguistics (p. 32)
Mass surveillance > Video surveillance (p. 40)

Biometric concealment includes any practice that obscures biometric identifiers (unique physical or biological characteristics) that can be used for identification purposes.

See the facial recognition topic[40] and the chapter "Traces" in Prisma[102].

5.9. Bug search

Techniques addressed by this mitigation:

Covert surveillance devices > Audio (p. 21)
Covert surveillance devices > Location (p. 21)
Covert surveillance devices > Video (p. 23)
Targeted digital surveillance > Authentication bypass (p. 49)
Targeted digital surveillance > IMSI-catcher (p. 50)

Searching for bugs is the active process of trying to detect the presence of **covert surveillance devices (p. 20)** in a building, vehicle, or outdoor area. The primary technique in this process is a manual, visual search of the area. A secondary technique is to use specialized detection equipment.

Searching for bugs in a comprehensive and effective manner requires an extreme degree of technical expertise. If you do not have that expertise, when searching for bugs in an area, you cannot be sure that you have found all the bugs present in the area. Therefore, the purpose of searching for bugs should be to prevent an adversary from gathering information about you, not to consider an area free of covert surveillance devices. Incriminating conversations should always take place **outdoors and without digital devices (p. 69)**.

The primary technique when searching for bugs in an area is a manual, visual search of the area:

- If you're searching a building, you can use appropriate tools to disassemble electrical outlets, multiple-socket adapters, ceiling lights, and any electrical appliances, looking for anything that shouldn't be there. You can also look inside furniture, basically anywhere a bug might fit.
- If you're searching a vehicle, you can look under the vehicle, inside the wheels, on the rear bumper, behind the vents, looking for anything that shouldn't be there. You can use appropriate tools to dismantle the interior, the ceiling, the dashboard, the seat heads, and so on. On motorcycles or bikes, you can look inside or under the seats. Unlike other vehicles, when searching a **bike (p. 75)**, you can determine with a high degree of confidence whether or not a bug is present.
- If you're searching for cameras installed at the windows of buildings on a street, you may be able to see such cameras with binoculars.
- If you're searching for cameras installed in surveillance vehicles on a street, you can detect such vehicles with **passive surveillance detection (p. 73)**.

A secondary technique when searching for bugs is to use specialized detection equipment. Such equipment can be purchased at specialty stores or on the Internet, and includes:

- Radio frequency detectors, to detect devices that are transmitting data on radio frequencies at the time of the search.
- Camera lens detectors to detect cameras.
- Professional equipment—spectrum analyzers, non-linear junction detectors, thermal imaging systems—which can be more effective, but is very expensive and complex to use.

See Ears and Eyes[12] for a database of cases of covert surveillance devices used against anarchists and other rebels.

5.10. Careful action planning

Techniques addressed by this mitigation:

Canine trackers (p. 19)
Forensics > Arson (p. 26)
Forensics > DNA (p. 27)
Forensics > Fingerprints (p. 30)
Forensics > Trace evidence (p. 32)
Increased police presence (p. 35)
Mass surveillance > Civilian snitches (p. 39)

Once you have all the information you need from the **reconnaissance (p. 72)** phase, it is time to make it actionable with a well-developed plan. Everyone involved needs to have a clear understanding of their role and how their tasks relate to everyone else's.

For example, what is the best route to and from the site, and how long will you be at the site, given the expected timing of a police response? Or, what on your escape route could interfere with a police pursuit (e.g. will police need to get out of their vehicle to follow on foot)? Creating an action plan is a form of threat modeling—what could go wrong, what mitigations will we implement, and how? For example, how will **anti-surveillance (p. 56)** be conducted prior to the action meeting point?

5.11. Clandestinity

Techniques addressed by this mitigation:

Covert house search (p. 20)
House raid (p. 34)

Clandestinity is the process of breaking away from your established identity and begin a new life with a **fake identity (p. 66)**.

You can enter clandestinity:

- In response to repression, for example to avoid imprisonment, or after an escape from prison.
- To participate in an clandestine organization, that is, an organization in which it has been decided that all members should enter clandestinity.

See the clandestinity topic[107].

5.12. Compartmentalization

Techniques addressed by this mitigation:

Network mapping (p. 42)
Targeted digital surveillance > Malware (p. 51)
Targeted digital surveillance > Network forensics (p. 52)

Compartmentalization is a security principle in which different identities (or projects) are kept separate so that they cannot be connected, and the compromise of one is isolated from the compromise of the others. This principle can be applied to both digital and non-digital identities.

Examples of digital compartmentalization include:

- Using different email accounts for different digital identities, such as one account for work, another for friends, another for a specific sensitive project, etc. This way, if an adversary knows your work email address and discovers your sensitive email address after seizing a computer in a house raid, because the email addresses are different, they won't know that they belong to the same person.
- Using different Tails[39] USB sticks or Qubes OS[94] virtual machines for different digital identities. This way, if an adversary compromises one stick or virtual machine with **malware (p. 49)**, the compromise won't spread to other sticks or virtual machines.

Examples of non-digital compartmentalization include:

- Using different names in different contexts, such as using your civil name with your family but an alias with your friends. An alias can be specific to a place, time, or group of people you interact with. This way, if an adversary compromises one of your names, it won't necessarily lead to the compromise of the others.
- Applying the **need-to-know principle (p. 68)** by sharing sensitive information only when it is necessary to do so, and only to the extent necessary.

Compartmentalization can be a useful tool for remembering to apply mitigations consistently within a project. For example, you may want to always take **anti-surveillance (p. 56)** measures when traveling as part of a specific project, but not make the same effort for another, less sensitive project.

[107] https://notrace.how/resources/#topic=clandestinity

5.13. Computer and mobile forensics

Techniques addressed by this mitigation:

Targeted digital surveillance > Malware (p. 51)
Targeted digital surveillance > Physical access (p. 53)

Computer and mobile forensics is a highly technical discipline aimed at identifying a compromise on a computer or phone. False negatives are common.

See also:

- The Device Integrity[108] page on Privacy Guides.
- Practical Linux Forensics[109] for a comprehensive introduction to the skill set on Linux, the platform most relevant to anarchists and other rebels.

5.14. DNA minimization protocols

Techniques addressed by this mitigation:

Forensics > DNA (p. 27)

DNA minimization protocols allow you to manipulate objects while minimizing the amount of **DNA (p. 27)** you leave on them. Some protocols focus on never leaving DNA traces on an object in the first place. Other protocols focus on removing DNA traces from an object by chemically destroying DNA molecules.

DNA minimization protocols may involve:

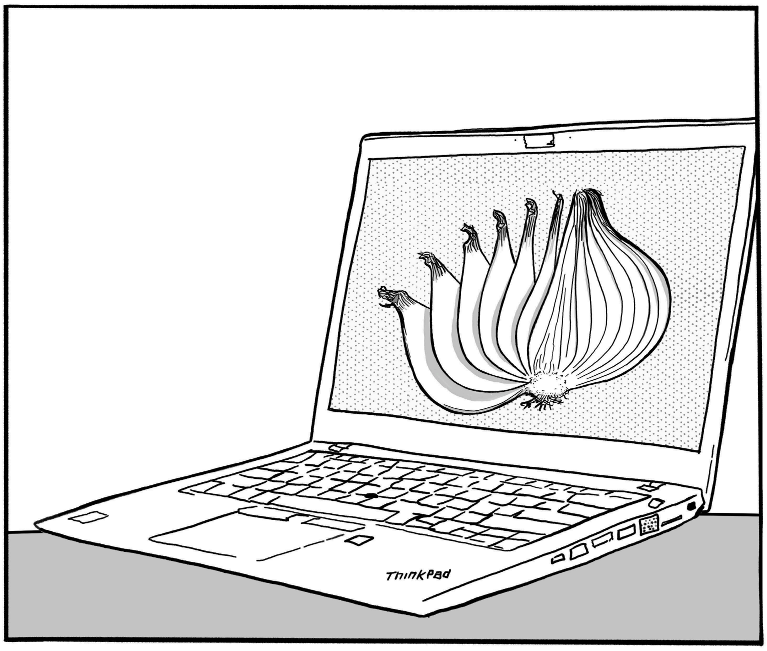
- Purchasing an object in individual plastic packaging so that you don't risk leaving DNA on it until you open the packaging.
- Manipulating an object while wearing a new pair of non-permeable gloves (e.g., dish washing gloves or thick work gloves) so that there are no DNA traces on the outside of the gloves that could be transferred to the object.

[108] https://privacyguides.org/en/device-integrity
[109] https://notrace.how/resources/#practical-linux-forensics

- Storing an object in a new, non-permeable garbage bag so that DNA from the environment doesn't contaminate the object during storage.
- Destroying DNA molecules with sodium hypochlorite, which is present in adequate concentrations in some brands of bleach.

See blabladn[25] for protocol suggestions, and the DNA topic[26].

5.15. Digital best practices



Techniques addressed by this mitigation:

Alarm systems (p. 19)
Covert surveillance devices > Video (p. 23)
Door knocks (p. 23)
Forensics > Digital (p. 29)
Mass surveillance > Mass digital surveillance (p. 39)
Network mapping (p. 42)
Service provider collaboration (p. 47)
Targeted digital surveillance > Authentication bypass (p. 49)
Targeted digital surveillance > Malware (p. 51)
Targeted digital surveillance > Network forensics (p. 52)
Targeted digital surveillance > Physical access (p. 53)

The foundation of digital best practices is to limit the reach of technology into your life. For example, if you have a mobile phone, leave it at home to avoid the possibility of location tracking. That said, digital devices should run open source and security-oriented operating systems and be configured with best practices in mind.

Do not use Windows, MacOS, iPhones, and stock Android. Use security-oriented operating systems:

- Debian[89] or Qubes OS[98] for daily computer use.
- Tails[39] for sensitive computer use, such as reading a sensitive article, researching for an action, writing and sending an action claim, and moderating a sketchy website. Tails is an operating system installed on a USB stick. It is unique in that it is designed for anonymity

and leaves no trace on your computer[110]. All Internet connections are forced through the Tor network[66], and everything runs in the computer's memory (which is irrecoverable after the computer is shut down). See the official website[39] for easy-to-use installation instructions and great documentation.
- GrapheneOS[111] for phones.

Enable **Full Disk Encryption (p. 65)** on all your digital devices.

Use strong passwords:

- Most of your passwords (e.g. passwords you use to log in to websites) should be generated by and stored in a password manager—we recommend KeePassXC[112]—so that you don't have to remember them or even type them. They can be very long and random, say 40 random characters. You can generate such passwords with KeePassXC (select the "Password" tab when generating a password).
- The passwords you enter when booting your encrypted devices and KeePassXC's password must be memorized. We recommend using Diceware[113] passwords of 5 to 7 words[114]. You can generate such passwords with KeePassXC (select the "Passphrase" tab when generating a password) or with physical dice[115]. You should use different passwords for each of your encrypted devices, but you can use the same password for all your KeePassXC databases.

For example, if you have an encrypted laptop, a Tails stick and an encrypted phone, you will have to remember 4 passwords of 5 to 7 words (one for each device and one for the KeePassXC databases). This is a lot! To make sure you don't forget all those passwords, you can:

- Use memorization techniques, such as repeating the passwords in your head every day when you wake up.
- Store a copy of the passwords on a USB stick that you keep in a hidden place outside your home, and that is encrypted with a 7-word Diceware password. You don't memorize this 7-word password, you store it in the KeePassXC databases of one or two trusted comrades who also follow these digital best practices. This way, if you forget a password, you can ask the trusted comrades for the 7-word password and retrieve the USB stick: on it, you will find the forgotten password.
- Store a copy of the passwords on a USB stick that you keep in a hidden place outside your home, and that is encrypted with a 14-word Diceware password. You don't memorize this 14-word password, you split it into two halves of 7 words each, write each half on a piece of paper, and store each piece of paper in a different hidden place (not with the USB stick). This way, if you forget a password, you can retrieve the two pieces of paper, reconstruct the 14-word password, and retrieve the USB stick: on it, you will find the forgotten password.

Use Tor[66] or a reputable Virtual Private Network (VPN) for your Internet activity:

- All of your sensitive Internet activity, and as much of your non-sensitive Internet activity as possible, should be done through Tor. If you use Tor, an adversary monitoring your network

[110] https://tails.boum.org/about/index.en.html

[111] https://grapheneos.org

[112] https://keepassxc.org

[113] https://en.wikipedia.org/wiki/Diceware

[114] Use 5 words to be safe *right now*, and 7 words to be safer *in the future*. This recommendation is based on the assumption that you use the operating systems we recommend, on our best knowledge of our adversaries' capabilities, and on time[116] and cost[117] estimates of brute-forcing modern cryptosystems.

[116] https://blog.elcomsoft.com/2020/08/breaking-luks-encryption

[117] https://blog.1password.com/cracking-challenge-update

[115] https://www.eff.org/dice

traffic knows that you use Tor, but not what websites you visit or what you do on those websites.

- Your non-sensitive Internet activity can be done through a reputable VPN. If you use a VPN, your Internet Service Provider cannot log the websites you visit and it is harder to target you with **malware (p. 51)**.

Use end-to-end encrypted messaging applications for your digital communications:

- Ideally, use decentralized and metadata-resistant applications such as Cwtch[84] or Briar[85].
- Email is not metadata-resistant and should be avoided if possible. If you must use email, use PGP encryption and register an address with a trusted service provider[83].

Back up your digital data regularly, especially data you really don't want to lose, such as your password manager database. Encrypt your backups with **Full Disk Encryption (p. 65)**. A typical practice is to have two backups:

- An "on-site" backup that you keep at home and update regularly, such as once a week.
- An "off-site" backup that you keep outside your home and update less frequently, such as once a month.

The advantage of the on-site backup is that it has a more recent version of your data. The advantage of the off-site backup is that it cannot be seized in the event of a **house raid (p. 34)** against your home.

5.16. Encryption

Techniques addressed by this mitigation:

Forensics > Digital (p. 29)
Mass surveillance > Mass digital surveillance (p. 39)
Service provider collaboration (p. 47)
Targeted digital surveillance > IMSI-catcher (p. 50)
Targeted digital surveillance > Malware (p. 51)
Targeted digital surveillance > Network forensics (p. 52)

Encryption is a process that renders data unintelligible to anyone who doesn't have the decryption key (often a password). Encryption can be applied to data "at rest" (such as files stored on your computer) and data "in motion" (such as messages in a messaging application).

You can encrypt "at rest" data on a digital device by enabling Full Disk Encryption (FDE) on the device with a **strong password (p. 63)**. When the device is turned off, its data is encrypted; when you turn it on and enter the decryption key, its data is decrypted until it is turned off. If a device with FDE enabled is seized by an adversary during an arrest, **house raid (p. 34)**, or **covert house search (p. 20)** while it is turned off, the adversary will not be able to access its data (unless they **bypass its authentication (p. 49)**).

You can encrypt "in motion" data by using Tor[66] or a Virtual Private Network (VPN) for your Internet activity, and by using **end-to-end encrypted messaging applications (p. 63)** for your digital communications. Encrypting "in motion" data can prevent an adversary from monitoring your digital activity in various ways.

Encryption should be considered a harm-reduction measure, not a panacea. Any incriminating activity should not be done on a digital device unless it's unavoidable, and incriminating conversations should take place **outdoors and without digital devices (p. 69)**.

5.17. Fake ID

Techniques addressed by this mitigation:

ID checks (p. 35)
Network mapping (p. 42)

A fake ID (short for *fake identity*) is an identity you assume in place of your established identity to avoid detection by an adversary. You can have multiple fake IDs, and you can switch between your established identity and your fake IDs depending on the context.

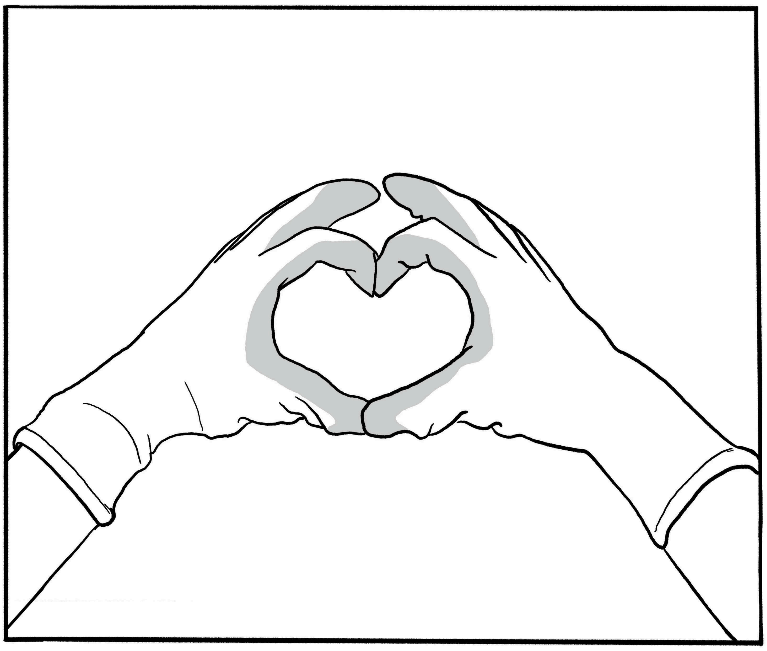
A fake ID can consist of:

- A fake name, place and date of birth, and other biographical information.
- A fake family history, employment history, and other background information.
- Fake identity documents.

You can use a fake ID:

- To prevent **network mapping (p. 42)** or avoid arrest in the event of an **ID check (p. 35)**.
- To establish a **safe house (p. 72)**.
- To take the path of **clandestinity (p. 61)**.

5.18. Gloves



Techniques addressed by this mitigation:

Forensics > DNA (p. 27)
Forensics > Fingerprints (p. 30)

Certain types of gloves can prevent you from leaving fingerprints on objects you touch and can hide hand characteristics such as skin color or tattoos. Gloves that are too thin are useless because they don't prevent you from leaving fingerprints (e.g. surgical gloves). Gloves made of certain materials are dangerous because they transfer fingerprints between objects (e.g. latex or leather gloves).

Always use gloves to handle any tools you bring with you to an action so you don't leave fingerprints on them. Although acetone can be used to remove fingerprints from surfaces, it is easier to avoid leaving fingerprints on something in the first place than to rely on removing them with an acetone-soaked cloth, which can be less effective on some types of surfaces. For example, on some surfaces, such as metal, the reaction between the finger grease and the metal can etch a print into the surface itself that can only be effectively removed with sandpaper.

Gloves can also prevent DNA from being left on objects you touch. The best gloves against DNA are non-permeable, such as a new pair of dishwashing gloves that cover the wrist area. Before putting on the gloves, thumb holes can be made in long sleeves of a shirt to prevent the sleeve from riding up during use and exposing arm hair and skin. Dishwashing gloves are not appropriate in a context such as a demonstration—use a new pair of work gloves that have a thick impermeable coating on the palms and fingers. All gloves transfer DNA traces between objects, so you need to put them on carefully and not touch your skin afterwards—see the related mitigation **DNA minimization protocols (p. 62)**.

In addition, fingerprints (and DNA) can be left on the inside of gloves, so you should dispose of them properly.

See the fingerprints topic[41] and Handschuhe[118] (in German).

5.19. Masking your writing style

Techniques addressed by this mitigation:

Forensics > Linguistics (p. 32)

To counter author identification by **forensic linguistics (p. 32)**, your writing style can be obscured by writing with brevity and intent.

A text can be checked for spelling and grammatical errors before publication to ensure that it does not contain unique errors that could be traced back to you.

To identify someone as the author of a text, an enemy can look for samples of that person's writing to use for comparison. To counter this, you can avoid keeping unencrypted samples of your writing at home that might be found in a **house raid (p. 34)**, and generally avoid publishing texts in your name throughout your life.

See Counteracting Forensic Linguistics[46] and Who wrote that?[47].

5.20. Metadata erasure and resistance

Techniques addressed by this mitigation:

Forensics > Digital (p. 29)

Metadata is data about data, i.e. information about other information. Metadata erasure is the removal of metadata. Metadata resistance is the ability of a digital system not to create metadata in the first place, or to encrypt the metadata it creates so that it cannot be read by an adversary.

Examples of metadata include:

- An image file can embed information about when it was taken and the camera or phone that took it.
- A PDF file can embed information about the computer that created it.
- An email embeds the email address that sent it and the email address that received it.

[118] https://militanz.blackblogs.org/163-2

- A printed document often has an invisible watermark[119] that identifies the make and model of the printer that printed it.

For digital files, metadata erasure can be accomplished using MAT2[120] or similar software. Some **security-oriented operating systems (p. 63)** include metadata erasure tools by default.

Examples of metadata resistance include:

- Using a dedicated operating system (e.g. a Tails[39] stick) to create or modify digital files so that information about the operating system you normally use is not embedded in the metadata of the files.
- Using metadata-resistant messaging applications such as Cwtch[84] or Briar[85].

5.21. Need-to-know principle

Techniques addressed by this mitigation:

Evidence fabrication (p. 24)
Infiltrators (p. 36)
Informants (p. 37)
Network mapping (p. 42)

The need-to-know principle means that sensitive information should be shared only when it is necessary to do so, and only to the extent necessary. This makes repression more difficult by controlling the flow of information through networks to make them more opaque to outsiders and harder to disrupt. Bragging about sensitive information violates the need-to-know principle.

For example, people who are not involved in an action should not know about it. People who have a specific and limited role in an action may not need to know who else is involved other than the person with whom they are communicating directly.

One coordinating structure that embodies this principle is the "spokes council": people from different affinity groups meet for a project without revealing to each other everyone involved. This principle should be weighed against its tendency to create "choke-points" of coordination —if one person is always the coordinating bridge between affinity groups, this can lend itself to a gate-keeping dynamic, as well as making further coordination impossible in the scenario of that person's imprisonment.

See the security culture topic[121].

5.22. Network map exercise

Techniques addressed by this mitigation:

Infiltrators (p. 36)
Informants (p. 37)
Network mapping (p. 42)
Targeted digital surveillance > Physical access (p. 53)

A network map exercise consists of creating a graphical representation of the links between you and the people in your network in order to critically examine those links. This exercise is designed to sharpen your ability to make informed and critical choices about the people you as-

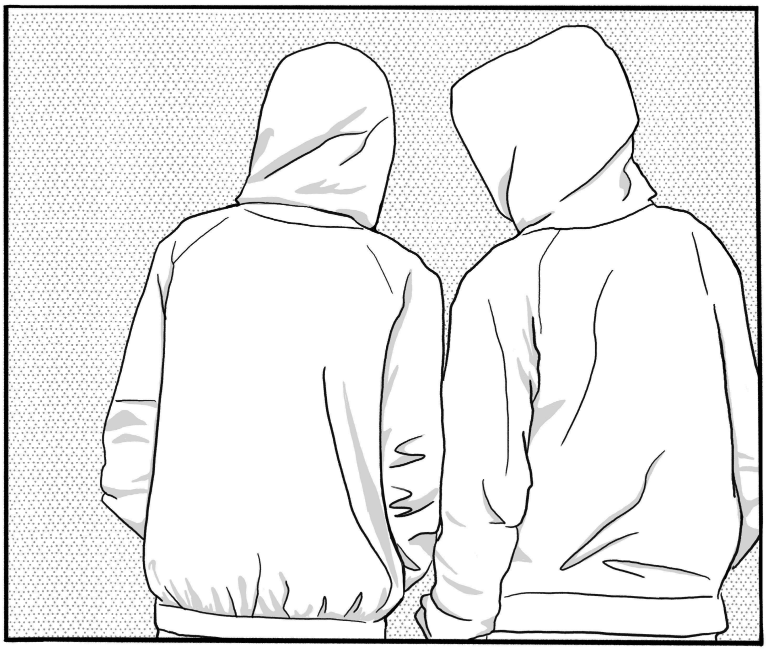
[119] https://eff.org/issues/printers
[120] https://github.com/tpet/mat2
[121] https://notrace.how/resources/#topic=security-culture

sociate with, with the ultimate goal of making your network more resilient to **infiltration (p. 36)** attempts.

A core idea of this exercise is to help you think not just at the level of your affinity groups, but at a more global level that includes people you don't know well, and may even include people you don't really know at all. It works by asking yourself a series of structured questions that reveal your level of security with all the people in your network, from which you draw a map that distinguishes the people you trust from the people you would like to know more about. It is designed to be done in times of relative calm.

For instructions on how to do this, see Stop hunting sheep: a guide to creating safer networks[56]. Such a network map would be invaluable to an enemy; it is essentially what they construct during **network mapping (p. 42)**, so it should be burned immediately after use.

5.23. Outdoor and device-free conversations



Techniques addressed by this mitigation:

Covert surveillance devices > Audio (p. 21)
Mass surveillance > Video surveillance (p. 40)

It is not possible to assume that indoor spaces, including cars, are free of **covert surveillance devices (p. 20)**, even after an exhaustive **bug search (p. 59)**. It is not possible to assume that electronic devices are free of **targeted malware (p. 51)** that could turn them into covert microphones. Therefore, all sensitive or incriminating conversations should be conducted outdoors and without electronic devices.

Outdoor conversations can be recorded with covert microphones or long-range parabolic microphones during a **physical surveillance (p. 43)** operation (with effective ranges of up to 300 meters). For example, in Italy in 2019[122], a microphone was hidden in a fake stone in front of a prison where gatherings were often held. As a result, it is best to conduct sensitive discussions while walking, or for larger group discussions where it would be too difficult to move, to hold them in spaces that change regularly and are difficult to place under audio surveillance.

[122] https://notrace.how/earsandeyes/#cuneo-2019-06

The practice of turning off mobile phones, removing their batteries, or placing them in Faraday bags during outdoor conversations generates **metadata (p. 67)** about who is having sensitive conversations, when, and where—it is best to simply leave such devices at home. In addition, a Faraday bag does nothing to prevent audio from being captured, only from being transmitted, which could happen when the phone later reconnects to the network.

See the security culture topic[121].

5.24. Physical intrusion detection

Techniques addressed by this mitigation:

Covert house search (p. 20)
Covert surveillance devices > Audio (p. 21)
Covert surveillance devices > Location (p. 21)
Covert surveillance devices > Video (p. 23)
Evidence fabrication (p. 24)
Targeted digital surveillance > Physical access (p. 53)

Physical intrusion detection is the process of detecting when an adversary enters or attempts to enter a space, for example for a **covert house search (p. 20)**. You can do this by making sure there is always someone in the space who would notice if an adversary tried to enter, or by monitoring the space with a video surveillance system.

A video surveillance system that monitors a space can have the following characteristics:

- The cameras can be motion-activated and send you an alert if they are detected and tampered with.
- The cameras can be positioned with the space entrances in their line of sight and/or in a discreet location.
- To prevent the system from monitoring you while you are in the space, you can turn it on just before you leave the space and turn it off as soon as you return.

5.25. Preparing for house raids

Techniques addressed by this mitigation:

Covert house search (p. 20)
House raid (p. 34)

Preparing for house raids is the process of taking precautionary measures to minimize the impact of a potential **house raid (p. 34)** or **covert house search (p. 20)**.

An important precautionary measure is to minimize the presence of materials that you wouldn't want to be found by an adversary during a raid. In particular:

- All phones and computers should have **Full Disk Encryption (p. 65)** and be turned off overnight or when you are away for the encryption to be effective.
- Materials used in actions that can appear to have a “legitimate” purpose should be stored where they belong and not together (gloves with cleaning supplies, etc.)
- Materials used in actions that do not have a “legitimate” purpose should be kept in a **stash spot or safe house (p. 72)**, or at worst should only pass through the house for a very limited amount of time. In most contexts, we do not think it makes sense to avoid keeping anarchist literature at home, but specific guides to sketchy things should be avoided.

5.26. Preparing for repression

Techniques addressed by this mitigation:

Extra-legal violence (p. 25)

House raid (p. 34)

Preparing for repression is the process of taking precautionary measures to minimize the impact of repression. Repression often hits hardest when we're least prepared. Such preparation may seem emotionally draining, but we find that it actually allows us to act more freely. Preparing for repression can have practical or psychological dimensions.

Examples of practical preparation include:

- Ensuring that your comrades know what to do in the event of your arrest, for example by sharing a work email login or a house key in advance, arranging for people to care for children or pay your rent or bail, etc.
- Ensuring that your projects can continue if you are incarcerated, which can sometimes be as simple as sharing a password in advance.
- Training in martial arts to be better equipped to deal with the prisoner-on-prisoner violence that is prevalent in many prisons.
- If drug possession is highly criminalized in your context, you can stay away from illegal drugs. A State adversary can use drug charges to put pressure on you for the crimes they are really interested in.

Examples of psychological preparation include:

- Talking with comrades who have been the target of repression about their experiences, including their experiences of imprisonment.
- An experience described in Claudio Lavazza's autobiography[123] where he secluded himself in a house in the mountains for a month to prepare for the possibility of his imprisonment.

5.27. Prisoner support

Techniques addressed by this mitigation:

Informants (p. 37)

Prisoner support is the crucial process of organizing material, logistical, and emotional support for comrades behind bars. Beyond the ethical imperative to support our prisoners, people are less likely to turn informant if they feel supported and connected to the movements for which they risked their freedom.

Common prisoner support initiatives include:

- Writing letters.
- Providing financial support to prisoners or their close ones.
- Continuing projects or struggles that imprisoned comrades are unable to participate in because of their situation, and generally showing solidarity in ways that are meaningful to the comrades behind bars.
- Helping prisoners escape from prison.

[123] https://compasseditions.noblogs.org/post/2020/09/05/my-pestiferous-life-claudio-lavazza

5.28. Reconnaissance

Techniques addressed by this mitigation:

Alarm systems (p. 19)
Guards (p. 33)
Mass surveillance > Video surveillance (p. 40)
Police patrols (p. 47)

Reconnaissance is the gathering of information about the target of an action. It precedes **action planning (p. 60)**. It can be done either physically (e.g., by traveling to the action site to inspect it) or digitally (e.g., by researching the target on the web). You should take into account the techniques an adversary may use against you during reconnaissance as much as you take them into account during the action itself.

Examples of physical reconnaissance include:

- Inspecting possible routes to and from the action site to evaluate which route you might take. For example, a good route may have minimal **surveillance camera (p. 40)** coverage and a suitable place to change clothing before the action.
- Inspecting the action site itself, looking for surveillance cameras, **guards (p. 33)**, **alarm systems (p. 19)** and opportunities to attack the target.

When conducting physical reconnaissance, you can:

- Practice **anti-surveillance (p. 56)** to counter the risk of physical surveillance.
- **Dress anonymously (p. 54)** to counter the risk of being observed or recorded.

Examples of digital reconnaissance include:

- Visiting the target's website.
- Inspecting the action site on online maps.

When conducting digital reconnaissance, you should follow **digital best practices (p. 63)**.

5.29. Stash spot or safe house

Techniques addressed by this mitigation:

Covert house search (p. 20)
Covert surveillance devices > Video (p. 23)
Forensics > Ballistics (p. 26)
Forensics > Trace evidence (p. 32)
House raid (p. 34)

Stash spots and safe houses are two ways to store incriminating materials. If incriminating materials are stored in a stash spot or safe house instead of in your home, they won't be found by an adversary in the event of a **house raid (p. 34)** or **covert house search (p. 20)**. A stash spot is a hidden place, often outdoors, that is unlikely to be stumbled upon. A safe house is a house, apartment, or other space that an adversary doesn't know you're using.

Stash spots and safe houses each have advantages and disadvantages:

- It is easier to set up a stash spot.
- It is easier to **minimize DNA traces (p. 62)** in a stash spot.
- It is easier to change the location of a stash spot.

- A safe house provides more storage space and can be used for purposes other than storage such as sleeping, preparing materials, etc.

Examples of stash spots include:

- A box buried in a wooded area far from a trail (so hikers don't risk stumbling upon it).
- A hidden place in an abandoned building tucked away somewhere.

Examples of safe houses include:

- A house, apartment, or other space rented with a **fake ID (p. 66)** and cash.
- The home of someone you trust and who willing to take the risk this complicity entails, but who is far enough away from networks that are under surveillance.

If an adversary finds out about a stash spot or safe house, they can start monitoring it in order to identify you when you access it, as has happened in Italy, where motion-activated hunting cameras were installed to monitor a forest stash spot[124]. Because of this, when accessing a stash spot or safe house, you can:

- Practice **anti-surveillance (p. 56)** to counter the risk of physical surveillance.
- **Dress anonymously (p. 54)** to counter the risk of being observed or recorded.
- Practice **tamper-evident preparation (p. 74)** to ensure that the stash spot or safe house hasn't been accessed by an adversary.

5.30. Surveillance detection

Techniques addressed by this mitigation:

Covert surveillance devices > Video (p. 23)
Physical surveillance > Aerial (p. 44)
Physical surveillance > Mobile (p. 45)

Surveillance detection is the practice of detecting if you are under **physical surveillance (p. 43)**, that is, detecting if you are being directly observed by an adversary. There are two types of surveillance detection: passive surveillance detection and active surveillance detection. Counter-surveillance is a sophisticated form of active surveillance detection.

Passive surveillance detection is when you detect surveillance without deviating from your normal routine. Examples of passive surveillance detection include:

- Regularly checking the rear and side view mirrors while in a moving vehicle to detect surveillance vehicles following you.
- Listening to the sounds around you to detect drones or helicopters flying overhead.

Active surveillance detection is when you detect surveillance by doing something outside of your normal routine in an attempt to force a potential surveillance effort to reveal itself. Examples of active surveillance detection include:

- Taking an illogical route to travel between two points, such as a route that isn't the shortest route. If a pedestrian or vehicle takes the same illogical route as you, they may be a surveillance operator. If possible, you should have a valid reason for taking this illogical route (such as stopping at a store along the route), so that a surveillance effort doesn't notice that you are conducting surveillance detection.

[124] https://actforfree.noblogs.org/post/2022/06/24/italy-youll-find-us-in-our-place-as-we-cant-stay-in-yours-on-the-diamante-investigation

- Making an unexpected U-turn while driving. If you are being followed by an incompetent surveillance team (or a single surveillance vehicle), a surveillance vehicle may mirror your U-turn, which is a clear sign that they are following you. If you are being followed by a competent multi-vehicle surveillance team, the surveillance vehicles will not mirror your U-turn, as this would be suspicious, but your unexpected U-turn can still elicit unnatural reactions from them, which can help you to detect them. If possible, you should have a valid reason for making the U-turn, so that a surveillance effort doesn't notice that you are conducting surveillance detection.

Counter-surveillance is when you detect surveillance with the help of a trusted third party (i.e., one or more people) who is presumably not under surveillance, and who attempts to detect if you are under surveillance. The following is an example of a counter-surveillance operation:

1. Select a route that you will take during the counter-surveillance operation. The route should appear logical to a potential surveillance effort, but should be illogical for anyone else to take, and should include several stops that are suitable for the third party to attempt to detect a surveillance effort. For example, you can start at your home, stop at three or four hardware stores in your city pretending to price a certain item, and return to your home. This route would appear logical to a potential surveillance effort, but it is unlikely that anyone else would take the same route, stopping at the same stores in the same order as you.
2. As you follow the selected route, the third party ensures that they are present at each stop before you, but without taking the same route as you (so they won't detected by a potential surveillance effort). To accomplish this, the third party can use a faster mode of travel than you, or leave each stop before you to get a head start, or use multiple coordinated teams.
3. At each stop, the third party takes note of pedestrians and vehicles arriving after you. If the third party notices that a pedestrian or vehicle is present at two or more stops, they may be part of a surveillance effort. The third party can also detect behaviors typical of surveillance operators, such as transmitting information through a radio hidden on their body, communicating with each other through visual signals, running unexpectedly, etc.

If an adversary notices that you are conducting surveillance detection, they may adapt and become more discreet. Therefore, when conducting surveillance detection, you should avoid revealing that you are doing so, if possible. If you successfully detect surveillance, you should avoid visibly acknowledging or evading the surveillance effort.

See the physical surveillance topic[80] and the related mitigation **Anti-surveillance (p. 56)**.

5.31. Tamper-evident preparation

Techniques addressed by this mitigation:

Targeted digital surveillance > Authentication bypass (p. 49)
Targeted digital surveillance > Physical access (p. 53)

Tamper-evident preparation is the process of taking precautionary measures to make it possible to detect when something has been **physically accessed (p. 53)** by an adversary.

Tamper-evident preparation can be used:

- To detect if an adversary has accessed an electronic device during a **covert house search (p. 20)** (in which case they may have installed **malware (p. 51)** on the device).
- To detect if an adversary has accessed a **stash spot or safe house (p. 72)**.

Examples of tamper-evident preparation techniques include:

- Applying nail polish to a laptop screws and taking pictures of the screws. Because nail polish has a complex pattern, it will be very difficult for an adversary to remove the screws without altering the pattern. Therefore, when you want to verify that the laptop has not been opened, you can take new pictures of the screws and compare them with the original pictures: if the nail polish patterns are identical, it means that the laptop has not been opened.
- Immersing electronic devices in a transparent box filled with a mixture of small objects of different colors (for example, half black pebbles and half white pebbles) and taking pictures of the sides of the box. Because such a mixture has a complex pattern, it will be very difficult for an adversary to remove the electronic devices without altering the pattern. Therefore, when you need to remove the electronic devices from the box, you can take new pictures of the sides of the box and compare them with the original pictures: if the mixture patterns are identical, it means that the electronic devices have not been accessed. A systematic application of this technique is to ensure that an electronic device (e.g. a laptop) is always immersed in such a box when you're not near it.

5.32. Transportation by bike

Techniques addressed by this mitigation:

Covert surveillance devices > Location (p. 21)
Mass surveillance > Video surveillance (p. 40)
Physical surveillance > Mobile (p. 45)

Transportation by bike has several advantages over other modes of transportation.

Advantages of transportation by bike include:

- Bikes are more difficult to identify through **video surveillance (p. 40)** than cars: the make and model of a bike can be obscured and bikes usually have no license plates.
- It is harder for a **mobile physical surveillance effort (p. 45)** to follow a bike than a car or someone on foot, especially without being detected, and it is easier to conduct **surveillance detection (p. 73)** and **anti-surveillance (p. 56)** from a bike. For example, in a six-month **physical surveillance (p. 43)** operation against a comrade in France, the police regularly lost track of him while he was biking.
- There are far fewer places to install a **tracking device (p. 21)** on a bike than on a car, and when you **search (p. 59)** a bike, you can tell with a high degree of confidence whether a tracking device is present or not.

6. Repressive operations

6.1. Berlin 2023 railway conspiracy case

Countries: **Germany (p. 85)**
Date: 2023 - ?
Techniques used:

Physical surveillance > Aerial (p. 44)

In February 2023, a few minutes after midnight, during a routine surveillance flight, the helicopter of the German federal police identified two comrades on railroad tracks near Berlin[77]. Three police cars were dispatched to the location and the comrades were arrested on suspicion of attempted arson against the railway infrastructure.

6.2. Repression of Lafarge factory sabotage

Countries: **France (p. 85)**
Date: 2022 - ?
Techniques used:

Forensics > DNA (p. 27)
House raid (p. 34)
Mass surveillance > Video surveillance (p. 40)
Open-source intelligence (p. 43)
Targeted digital surveillance > Authentication bypass (p. 49)
Targeted digital surveillance > Malware (p. 51)

On June 5, 2023, about fifteen people were raided and arrested in France, accused of participating in the December 2022 sabotage of a factory of the French industrial company Lafarge[54]. The sabotage, which took place during the day and involved between 100 and 200 activists[125], caused around 6 million euros of damage.

On June 20, 2023, about eighteen more people were raided and arrested in France, some of them in connection with the Lafarge sabotage[126].

6.3. Repression of the first Jane's Revenge arson

Countries: **United States (p. 86)**
Date: 2022 - ?
Techniques used:

Forensics > DNA (p. 27)
Forensics > Handwriting analysis (p. 31)
Mass surveillance > Video surveillance (p. 40)
Physical surveillance > Mobile (p. 45)

[125] https://reporterre.net/Sabotage-de-l-usine-Lafarge-deux-premieres-mises-en-examen

[126] https://reporterre.net/Nouvelle-serie-de-perquisitions-a-la-zad-et-en-France

In March 2023, a comrade was arrested[127] and charged with a May 2022 arson attack on the headquarters of an anti-abortion group[128]. The arson was the first in a series of attacks claimed under the name "Jane's Revenge" (a reference to the "Jane Collective", an underground organization that facilitated access to abortion in the United States from 1969 to 1973).

6.4. Belarusian anarcho-partisans

Countries: **Belarus (p. 85)**
Date: 2020 - 2021
Techniques used:

Extra-legal violence (p. 25)
Mass surveillance > Civilian snitches (p. 39)

In 2020, four anarchists set fire to police buildings and vehicles in the parking lot of a prosecutor's office[129]. Soon after, they were arrested by border guards while trying to cross the Belarusian-Ukrainian border.

In the first days of their detention, the anarchists were tortured[23]. Eventually, all four took responsibility for carrying out the actions of which they were accused.

After a trial in 2021, they were sentenced to 18 to 20 years in prison[130].

6.5. Case against Boris

Countries: **France (p. 85)**
Date: 2020 - 2021
Techniques used:

Covert surveillance devices > Location (p. 21)
Covert surveillance devices > Video (p. 23)
Forensics > DNA (p. 27)
ID checks (p. 35)
Interrogation techniques (p. 38)
Mass surveillance > Police files (p. 40)
Mass surveillance > Video surveillance (p. 40)
Physical surveillance > Mobile (p. 45)
Service provider collaboration (p. 47)
Targeted digital surveillance > IMSI-catcher (p. 50)

In 2020, Boris, an anarchist from France, was accused of sabotaging a cell tower in Besançon, Doubs, France, in March 2020, and two cell towers on Mount Poupet in the Jura Mountains, France, in April 2020[18]. He was initially suspected when his DNA was found on a bottle cap at the foot of one of the burnt cell towers on Mount Poupet. The charges against him for the sabotage of the Besançon cell tower were later dropped for lack of evidence.

In a trial in 2021, Boris was sentenced to four years for the sabotage on Mount Poupet, with two to be served in prison and two on probation. After his trial, he publicly claimed responsibility for the sabotage in a text entitled "Why I burned the two antennas on Mount Poupet"[131].

[127] https://www.washingtontimes.com/news/2023/mar/28/hridindu-sankar-roychowdhury-arrested-charged-fire

[128] https://janesrevenge.noblogs.org/2022/05/08/first-communique

[129] https://pramen.io/en/2020/11/open-letter-in-support-of-belarus-anarchist-revolutionaries

[130] https://abc-belarus.org/en/2021/12/22/18-to-20-years-imprisonment-for-belarusian-anarcho-partisans

[131] https://anarchistnews.org/content/why-i-burned-2-antennas

6.6. 2019-2020 case against Mónica and Francesco

Countries: **Chile (p. 85)**
Date: 2019 - ?
Techniques used:

Forensics > DNA (p. 27)
Forensics > Facial recognition (p. 30)
Forensics > Handwriting analysis (p. 31)
Mass surveillance > Civilian snitches (p. 39)
Mass surveillance > Video surveillance (p. 40)
Open-source intelligence (p. 43)

In 2020, anarchists Mónica Caballero and Francisco Solar were arrested in Chile, accused of sending parcel bombs to a police station and a former Minister of the Interior in 2019, and placing bombs in a park in an attempt to harm cops in 2020[38]. Both have been charged with attempted murder.

In a trial in 2023, Francisco Solar was sentenced to 86 years in prison and Mónica Caballero to 12 years[132].

6.7. Repression against Zündlumpen

Countries: **Germany (p. 85)**
Date: 2019 - ?
Techniques used:

Forensics > DNA (p. 27)
Service provider collaboration (p. 47)
Targeted digital surveillance > Authentication bypass (p. 49)

In April 2022[91] and October 2022[133], several apartments and basements, a print shop, and a library were raided by police as part of an investigation into the alleged editors of the German anarchist newspaper *Zündlumpen*, published from 2019 to 2021.

During the April 2022 raid on the print shop, police seized thousands of books, zines, and newspapers, as well as all printing equipment and materials, apparently in an attempt to disrupt the printing capacity of local anarchists.

6.8. Repression of the 2019 uprising in Chile

Countries: **Chile (p. 85)**
Date: 2019 - 2020
Techniques used:

Extra-legal violence (p. 25)
Physical surveillance > Aerial (p. 44)

A series of protests and riots began in Chile in October 2019, following the announcement of an increase in the metro fare in Chile's capital, Santiago[134]. For several months, a large amount

[132] https://informativoanarquista.noblogs.org/post/2023/12/08/chile-condenas-contra-lxs-companerxs-monica-caballero-y-francisco-solar

[133] https://de.indymedia.org/node/234616

[134] https://crimethinc.com/2019/10/21/chile-resisting-under-martial-law-a-report-interview-and-call-to-action

of public infrastructure and commercial buildings were vandalized, looted or burned in Santiago and elsewhere in the country.

In response to the unrest, the government deployed soldiers and imposed a curfew in a number of cities[135]. Many people were arrested and sentenced to years in prison.

6.9. The three from the park bench

Countries: **Germany (p. 85)**
Date: 2019 - ?
Techniques used:
Mass surveillance > Video surveillance (p. 40)
Physical surveillance > Mobile (p. 45)

In 2019, three comrades were arrested while sitting on a park bench late at night in Hamburg[71], accused of carrying incendiary devices[136] and planning to burn down a specific building whose address was written on a piece of paper found on them. Two of the arrested comrades had been followed by cops for several hours before their arrest.

In a 2020 trial, the comrades were sentenced to between 19 and 22 months in prison[137]. The sentences were upheld on appeal in 2022[138].

6.10. Bialystok

Countries: **Italy (p. 85)**
Date: 2017 - 2022
Techniques used:
Forensics > Gait recognition (p. 31)
International cooperation (p. 38)

In June 2020, house raids took place in the *Bencivenga Occupato* squat in Rome and other places, and seven anarchist comrades were arrested in Italy, Spain and France as part of an operation called "Bialystok"[62]. They were accused of participating in an *associazione sovversiva* (criminal association) and of various minor offenses related to initiatives in solidarity with comrades accused in the **Panico operation (p. 80)**. Two of them were accused of carrying out an explosive attack on a police station in 2017 and an arson attack on cars linked to ENI (an Italian multinational oil and gas company) in 2019, respectively.

After a trial in 2022, some comrades were acquitted and some were sentenced to prison, with sentences ranging from 45 days to one year[139].

[135] https://www.anarchistnews.org/content/chile-anarchist-analysis

[136] https://parkbanksolidarity.blackblogs.org/509

[137] https://parkbanksolidarity.blackblogs.org/end-of-the-trial-two-imprisoned-comrades-on-the-streets-again

[138] https://zuendlappen.noblogs.org/post/2022/06/06/hamburg-einmal-schneller-sein-als-die-presse-die-revision-im-sog-parkbankverfahren-gegen-drei-anarchistinnen-aus-hamburg-ist-jetzt-abgeschlossen

[139] https://actforfree.noblogs.org/post/2022/10/31/italy-the-first-grade-sentence-concerning-the-trial-following-theoperation-bialystok

6.11. Network

Countries: **Russia (p. 86)**
Date: 2017 - 2020
Techniques used:

Extra-legal violence (p. 25)

In late 2017 and early 2018, about ten anarchists and antifascists were arrested in Penza and Saint Petersburg[21] and accused of being part of an underground organization called "Network" that was planning terrorist attacks in anticipation of the 2018 Russian presidential elections and the FIFA World Cup[140]. Some were also accused of attempting to sell large quantities of drugs. Most of them were tortured in the early stages of their detention by the Russian Federal Security Service (FSB).

According to the case files and other information, the initial arrests that launched the investigation were made because most of the defendants from Penza were involved in the drug business[141].

After two trials in 2020, seven alleged members of the "Network" organization in Penza were sentenced to prison terms ranging from 6 to 18 years[142], and two alleged members in Saint Petersburg were sentenced to 5 and a half and 7 years in prison, respectively[143].

6.12. Panico

Countries: **Italy (p. 85)**
Date: 2016 - 2023
Techniques used:

Forensics > DNA (p. 27)

In 2017, house raids took place in Florence and several anarchist comrades were arrested as part of an operation called "Panico"[62]. Up to 35 comrades were charged in this operation[144]. Some comrades were accused of carrying out an explosive attack on a fascist bookshop in 2017 and an arson attack on a police station in 2016. Other comrades were accused of various other actions.

After a trial in 2019, an appeal in 2021[145] and a ruling by the Court of Cassation in 2023[146], two comrades were sentenced to 8 years in prison, while others received sentences ranging from a few months to three and a half years.

6.13. Prometeo

Countries: **Italy (p. 85)**
Date: 2016 - 2021
Techniques used:

[140] https://www.amnesty.org/en/wp-content/uploads/2021/05/EUR4696252018ENGLISH.pdf

[141] https://web.archive.org/web/20210724130151/https://a2day.net/the-dark-side-of-the-network-case

[142] https://therussianreader.com/2020/02/10/network-penza-sentences

[143] https://anarchistsworldwide.noblogs.org/post/2020/06/23/saint-petersburg-russia-we-can-dance-if-we-want-to-sentencing-of-the-network-case-defendants

[144] https://insuscettibilediravvedimento.noblogs.org/post/2019/07/18/it-en-italia-richieste-di-condanna-al-processo-per-loperazione-panico

[145] https://ilrovescio.info/2021/05/05/sentenza-dappello-processo-panico

[146] https://lanemesi.noblogs.org/post/2023/07/15/sentenza-di-cassazione-del-processo-panico-14-luglio-2023

Forensics > DNA (p. 27)
Mass surveillance > Video surveillance (p. 40)
Service provider collaboration (p. 47)

In 2019, three anarchist comrades were arrested as part of an operation called "Prometeo"[62]. They were accused of sending parcel bombs to prosecutors and a director of the prison administration in 2017. One of the comrades was also accused of carrying out an arson attack on an ATM in 2016.

In 2021, the comrade accused of the ATM arson was sentenced to 5 years in prison, while all the comrades were acquitted (for lack of evidence[147]) for the parcel bombs, although one of them had spent two and a half years in prison before being acquitted.

6.14. Renata

Countries: **Italy (p. 85)**
Date: 2016 - 2019
Techniques used:
Covert surveillance devices > Audio (p. 21)
Extra-legal violence (p. 25)
Forensics > DNA (p. 27)
House raid (p. 34)

In February 2019, 50 house raids took place, mainly in Trentino, and seven anarchist comrades were arrested as part of an operation called "Renata"[62]. More comrades were arrested in May 2019. The arrested comrades were accused of participating in an *associazione sovversiva* (criminal association) and carrying out various arson and explosive attacks between 2016 and 2018, including an explosive attack on the headquarters of the right-wing political party "Lega Nord" in Treviso. Some comrades were also accused of forging documents.

In a trial in December 2019, several comrades were sentenced to prison, with sentences ranging from one year and nine months to two years and six months.

6.15. Scintilla

Countries: **Italy (p. 85)**
Date: 2015 - 2023
Techniques used:
Covert surveillance devices > Audio (p. 21)
Door knocks (p. 23)
Forensics > DNA (p. 27)
Forensics > Gait recognition (p. 31)
International cooperation (p. 38)

In February 2019, the *Asilo Occupato* squat in Turin was evicted and six anarchist comrades were arrested—a seventh comrade, Carla, went on the run—as part of an operation called "Scintilla"[62]. Some of them were accused of carrying out several arson and explosive attacks on migrant detention centers and other targets between 2015 and 2018[44]. Some of them were accused of publishing a zine called "I cieli bruciano" ("The skies are burning") which contained information about entities responsible for the management and maintenance of migrant detention centers.

[147] https://actforfree.noblogs.org/post/2021/10/06/italy-op-prometeo-beppe-robert-and-nat-acquitted

In May 2019, another comrade, Boba, was arrested and accused of setting fire to a prison building with a nautical flare during a gathering in front of the prison where the other comrades were detained[19]. In November 2019, another comrade, Peppe, was arrested and accused of sending a parcel bomb in 2016 to a company involved in the management of a migrant detention center[35]. In July 2020, Carla, who had been on the run since the first arrests, was arrested in France and extradited to Italy.

After a trial in 2021[148]–2023, several comrades were sentenced to prison, with sentences ranging from 1 year to 4 years and 2 months[149].

6.16. Nea Filadelphia case

Countries: **Greece (p. 85)**
Date: 2011 - 2016
Techniques used:

- **Forensics > DNA (p. 27)**
- **Physical surveillance > Mobile (p. 45)**

In 2013, several comrades were arrested in Nea Filadelphia, a suburb of Athens[81]. Four of them were accused of carrying out bank robberies[150] in 2011[36] and 2013[151].

After a trial in 2014, two comrades were sentenced to 16 years in prison[152]. After another trial in 2014[153] and an appeal in 2016[154], the other two were sentenced to 9 and 11 years in prison, respectively.

6.17. Mauvaises intentions

Countries: **France (p. 85)**
Date: 2006 - 2012
Techniques used:

- **Forensics > DNA (p. 27)**
- **Network mapping (p. 42)**
- **Physical surveillance > Overt (p. 46)**
- **Service provider collaboration (p. 47)**

In 2008, six comrades were arrested and charged with preparation of terrorist acts, possession or manufacture of explosive or incendiary devices, and arson or attempted arson—including an attempted arson of an electrical cabinet in 2006 and an attempted arson of a police tow truck in 2007[33]. This operation was documented by comrades in a series of zines entitled “Mauvaises intentions[155]”.

[148] https://roundrobin.info/2021/10/op-scintilla-inizio-del-processo-e-volantino

[149] https://ilrovescio.info/2023/01/18/torino-sentenza-di-primo-grado-del-processo-scintilla

[150] https://machorka.espivblogs.net/2013/11/06/concerning-the-arrests-of-comrades-in-nea-philadelphia-on-304-athens

[151] https://machorka.espivblogs.net/2016/02/26/appeal-trial-for-the-double-bank-robbery-velvendo-case-greece

[152] https://machorka.espivblogs.net/2014/10/02/announcement-of-sentences-in-the-velvedo-double-robbery-case-11014-athens

[153] https://abcsolidaritycell.espivblogs.net/archives/tag/g-naxakis

[154] https://anarhija.info/library/grecia-l-ultimo-aggiornamento-sul-processo-d-appello-per-rapina-a-pirgetos-con-anarchic-en

[155] https://notrace.how/resources/#mauvaises-intentions

After a trial in 2012, five comrades were sentenced to between one and three years in prison[156].

6.18. Scripta Manent

Countries: **Italy (p. 85)**
Date: 2003 - 2023
Techniques used:
Forensics > DNA (p. 27)
Forensics > Handwriting analysis (p. 31)
Forensics > Linguistics (p. 32)
House raid (p. 34)
Targeted digital surveillance > Malware (p. 51)

In 2016, 32 house raids took place in different regions of Italy and several anarchist comrades were arrested as part of an operation called "Scripta Manent"[62]. Up to 22 comrades were under investigation in this operation. They were accused of forming or participating in an *associazione sovversiva con finalità di terrorismo* (criminal association with the aim of terrorism), referring to attacks claimed by the *Federazione Anarchica Informale* (FAI, Informal Anarchist Federation) since 2003[157]. Some of them were accused of explosive attacks carried out between 2005 and 2016. Some of them were accused of *istigazione a delinquere* (incitement to commit a crime) for writing in the anarchist newspaper *Croce Nera Anarchica* (Anarchist Black Cross) or for running radical websites.

Scripta Manent combined the contents of several previous investigations.

A first trial took place in 2017-2019, an appeal in 2020, and two further verdicts in 2022[158] and 2023[159]. The final verdict is:

- Two comrades, Anna Beniamino and Alfredo Cospito, were sentenced to 17 years and 9 months and 23 years in prison, respectively.
- 11 comrades were sentenced to prison, with sentences ranging from 1 year and 9 months to 2 years and 6 months.
- The other comrades were acquitted.

6.19. Case against Jeff Luers

Countries: **United States (p. 86)**
Date: 2000 - 2008
Techniques used:
Forensics > Trace evidence (p. 32)
House raid (p. 34)
Physical surveillance > Mobile (p. 45)

On a night in June 2000, Jeff Luers and Craig Marshall were arrested in Oregon, United States, accused of setting fire to three trucks at a Chevrolet dealership earlier that night[49]. Jeff Luers was later also charged with an attempted arson of trucks at a petroleum products distributor in May 2000.

[156] https://juralib.noblogs.org/2012/06/25/mauvaises-intentions-paris-rendu-du-proces-antiterroriste-de-mai-2012

[157] https://tracesoffire.espivblogs.net/2016/09/13/italy-naples-september-carrion-operation-scripta-manent

[158] https://actforfree.noblogs.org/post/2022/07/10/italy-cassation-of-the-scripta-manent-trial

[159] https://actforfree.noblogs.org/post/2023/07/02/italy-anarchists-alfredo-cospito-and-anna-beniamino-have-been-sentenced-to-23-years-and-17-years-and-9-months

The June arson charge was based in part on a mobile physical surveillance operation conducted on the night of the arson. The May arson attempt charge was based in part on incendiary devices found intact at the site of the attempted arson and on the raid of a storage unit rented by Jeff Luers.

In a first trial, Jeff Luers was sentenced to 22 years and 8 months in prison, which was reduced to 10 years on appeal in 2008[160]. Craig Marshall was sentenced to 5 and a half years in a plea deal[161].

6.20. Case against Marius Mason

Countries: **United States (p. 86)**
Date: 1999 - 2010
Techniques used:
Informants (p. 37)

In 2008, Marius Mason was arrested and charged with several acts of arson and other vandalism claimed by the Earth Liberation Front (ELF) and the Animal Liberation Front (ALF)[59] from 1999 to 2003[162], including a 1999 arson of an office associated with Genetically Modified Organism (GMO) research.

In a 2009 trial, Marius Mason was sentenced to 21 years and 10 months in prison, a sentence that was upheld on appeal in 2010.

[160] https://machorka.espivblogs.net/2014/03/07/interview-with-convicted-eco-terrorist-jeff-free-luers-2008

[161] https://www.nytimes.com/2002/04/07/magazine/from-tree-hugger-to-terrorist.html

[162] https://supportmariusmason.org/wp-content/uploads/2016/08/mason-plea-agreement-1.pdf

7. Countries

7.1. Belarus

7.2. Chile

7.3. France

7.4. Germany

7.5. Greece

7.6. Italy

7.7. Russia

Repressive operations:

7.8. United States

Repressive operations:

8. Contribute to the Threat Library

8.1. Contact

Is there a **technique (p. 19)**, **mitigation (p. 54)**, or **repressive operation (p. 76)** that you think is missing? Would you like to edit one that is currently listed? To contribute to the Threat Library with additions, improvements, criticism, or feedback, get in touch with us:

notrace@autistici.org (PGP)

8.2. Repressive operations

The Threat Library aims to reference repressive operations that have targeted anarchists or other rebels anywhere in the world, and that feature interesting repressive techniques that are representative of local State repression. In order to diversify our coverage we are particularly looking for operations outside of Western Europe or North America, but we welcome contributions from these regions as well.

8.3. Translations

To coordinate translations across the No Trace Project, we use the Weblate collaborative localization platform. To translate the Threat Library into a new language, or to improve an existing translation, register an account on the Weblate instance used by the No Trace Project[163] (you will need an email address) and follow the instructions[164]. All languages are welcome.

[163] https://weblate.anarchyplanet.org

[164] https://weblate.anarchyplanet.org/projects/ntp/#information

The Threat Library is a knowledge base of repressive techniques used by the enemies of anarchists and other rebels and repressive operations where they've been used—a breakdown and classification of actions that can be used against us. Its purpose is to help you think through what mitigations to take in a particular project and to navigate resources that go into more depth on these topics. In other words, it helps you arrive at appropriate operational security for your threat model.

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.