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.

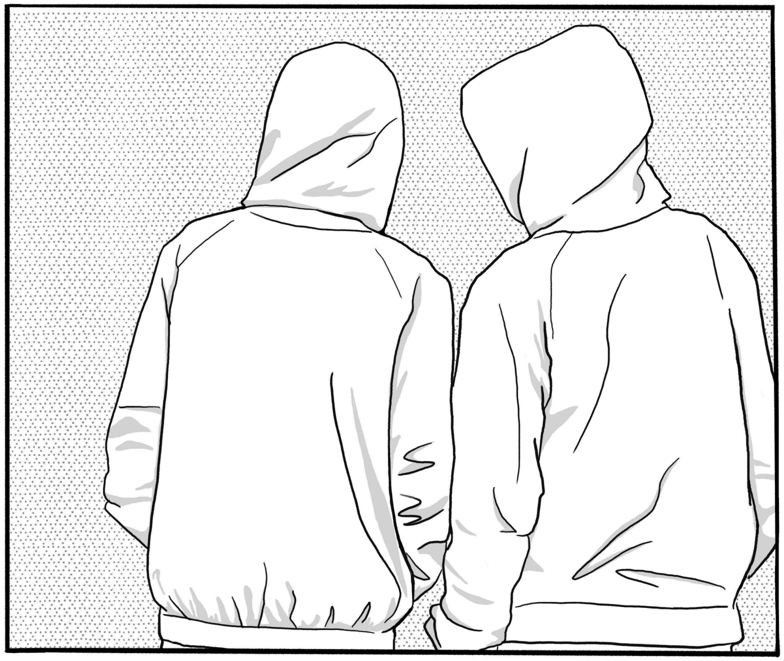
No Trace Project / No trace, no case. A collection of tools to help anarchists and other rebels **understand** the capabilities of their enemies, **undermine** surveillance efforts, and ultimately **act** without getting caught.

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.

Threat Library

Part 1/3

Tutorial, Tactics



Threat Library
Part 1/3: Tutorial, Tactics
Part 2/3: Techniques
Part 3/3: Mitigations, Repressive operations, Countries

Original publication by the No Trace Project

notrace.how/threat-library

This zine is divided into several parts. Sections in the current part are referenced by their page number. Sections in other parts are referenced by the # symbol followed by the part number.

April 11, 2024

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

- **Open-source intelligence (#2)**
- **Parallel construction (#2)**
- **Physical surveillance (#2)**
- **Police patrols (#2)**
- **Service provider collaboration (#2)**
- **Targeted digital surveillance (#2)**

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 (#2)**
- **Detection dogs (#2)**
- **Guards (#2)**
- **House raid (#2)**
- **ID checks (#2)**
- **Increased police presence (#2)**
- **International cooperation (#2)**
- **Police patrols (#2)**

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

3. Tactics

3.1. Deterrence

Uses techniques:

Door knocks (#2)
Extra-legal violence (#2)
Increased police presence (#2)
Mass surveillance (#2)
Police patrols (#2)

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:

Covert house search (#2)
Covert surveillance devices (#2)
Detection dogs (#2)
Door knocks (#2)
Evidence fabrication (#2)
Extra-legal violence (#2)
Forensics (#2)
House raid (#2)
ID checks (#2)
Infiltrators (#2)
Informants (#2)
International cooperation (#2)
Interrogation techniques (#2)
Mass surveillance (#2)
Network mapping (#2)

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. Threat modeling

Threat modeling is a process by which you identify potential *threats* posed by your *adversaries* so that you can then identify and prioritize the mitigations you can take to address those threats. The list of threats and their associated risks is called a *threat model.*

If you carry out subversive actions or projects, you're probably already used to thinking about how to minimize the risk posed by various threats. Threat modeling formalizes this thought process to make it more organized and systematic.

1.2. The Threat Library

The Threat Library is a tool developed by the No Trace Project to help anarchists and other rebels use threat modeling in their actions and projects. The Threat Library uses some technical terms that you'll want to become familiar with:

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

(#3) when committing arson, you become less vulnerable to DNA forensics.

2.3.5. Risk and local context

Understanding the habits and motivations of an adversary 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 (#3)** 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[5] 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 tree, 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.
- Attack trees for different types of projects.
- Translating the Threat Library to new languages.

See the **contribute section (#3)** for more information.

- Arrest tactic: Impact is determined by whether the target is successfully apprehended.

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 an adversary feels more threatened by it.

For example:

- In most contexts, 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.
- In most contexts, if the adversary is the State, actions that are classified as "terrorism" or "threats to national security" will receive an extraordinary amount of resources. The State may devote many resources to actions that took place during an uprising, because the uprising was seen as a threat to the integrity of the State.

2.3.4. Mitigations decrease risk

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

For example, you are vulnerable to DNA forensics because your body constantly sheds DNA. If you apply **DNA minimization protocols**

- An **adversary** is an entity that wants to prevent you from achieving your goals, from carrying out your actions and projects. Typically your adversary is the State, but depending on your context you may have other adversaries (e.g., fascist groups).
- A **technique** (or *threat*) is something an adversary does to prevent you from achieving your goals.
- A **mitigation** is something you do to lower the risk of a technique being successful.
- A **tactic** is an adversary's goal when using a technique. In the Threat Library, we organize techniques into three tactics: deterrence, incrimination and arrest.
- A **repressive operation** is a real instance of repression from a State against anarchists.
- An **action or project** is what you want to accomplish: organize for a riot, publish subversive literature, smash something, burn something…

The Threat Library contains a lot of information on State repressive techniques. This can have a paralyzing effect by making the State seem all-powerful. The State is not all-powerful[2]. The intent of the Threat Library is neither to minimize nor exaggerate the State's capabilities, but rather to understand its options and how those options are used in different contexts.

1.3. Explore the Threat Library

There are many ways to explore the Threat Library:

[2] In fact, the vast majority of anarchist direct actions are not successfully prosecuted. Frustrated investigators in Bremen, Germany[3], and Grenoble, France[4], have spoken to the media about their failure to repress any of the arsons that have taken place in both locations over the years, which they attribute to the mitigations taken by the arsonists.

[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

- The home page[5] provides an overview of all the tactics and techniques.
- The **techniques (#2)**, **mitigations (#3)**, and **repressive operations (#3)** are listed on their respective pages.
- The **Threat Library Tutorial (p. 6)** is designed to help you use the Threat Library in the context of a particular action or project.

1.4. Limitations

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. Struggles for freedom are not primarily a technical matter, but a social one, and have psychological and emotional effects. As much as possible, we encourage you to take time before, during and after an action to discuss with all the people involved and to make sure that everyone's emotional needs are taken into account.

The Threat Library attempts to be as comprehensive as possible in covering the threats that anarchists and other rebels may face, but it is intended to grow over time and will never be complete. This is especially true as adversaries may evolve with new and unforeseen techniques. To avoid a false sense of security from using the Threat Library, we encourage you to use other sources of knowledge, to remain critical, and to always consider your personal context when making important decisions.

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

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

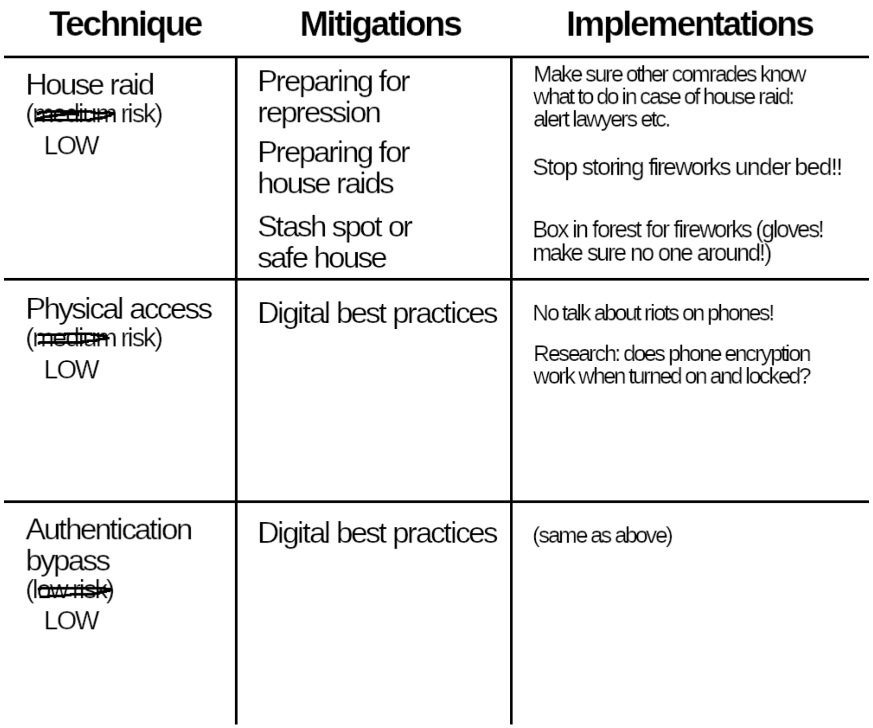
For example, in most contexts, if you are planning to commit arson, the **Forensics: DNA (#2)** technique is high risk. This is because it has a high impact (a good DNA match to an arson crime scene is solid evidence in court) and a high likelihood (in most contexts, DNA forensics is systematically used in arson investigations).

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.

[9] https://tails.net



Technique	Mitigations	Implementations
House raid (~~medium~~ risk) LOW	Preparing for repression	Make sure other comrades know what to do in case of house raid: alert lawyers etc.
	Preparing for house raids	Stop storing fireworks under bed!!
	Stash spot or safe house	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 your notes and then burn them. This approach makes it difficult to later revisit your notes and expand them.
2. At the end of the exercise, digitize your notes by manually copying them to an encrypted USB device using Tails[9] (remember to follow **digital best practices (#3)**). 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

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

There is a lot of information in the Threat Library. It can be overwhelming. How can you use the Threat Library in your life, in a particular project, or when carrying out actions? This tutorial is designed to help you navigate the Threat Library using *attack trees*[6].

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

You can do this *threat modeling* exercise on your own, but, if you're planning to carry out an action with other people, we recommend that you do it with them. This exercise should benefit both inexperienced and experienced crews. Even if everyone already has strong security practices, it provides a structured way to ensure that no threats are overlooked and that everyone is on the same page about security expectations.

2.1. A simple example: skipping a school day

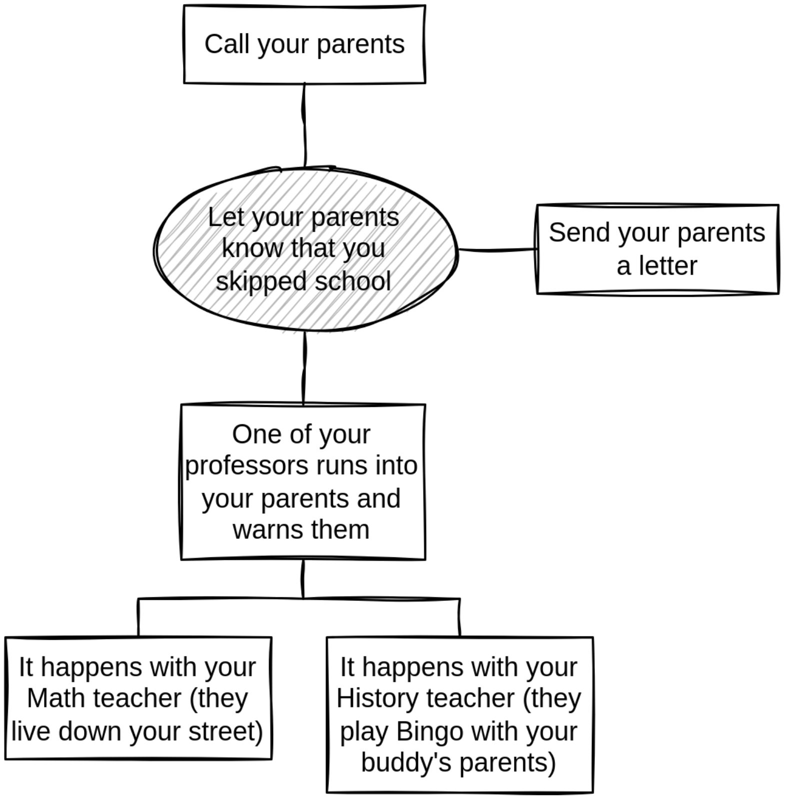
Let's start with a simple example before we consider a real one. You're a kid in school, and you and your buddy want to skip a day of school, but you don't want your parents to know. The adversary is the school system.

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

[6] For another approach to threat modeling that can also serve as a tutorial to the Threat Library, see Threat Modeling Fundamentals[7].

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

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. You draw all these nodes (1).


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 warns 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 for a node to be true, one of its successors must be true. For example, for “Let your parents know that you skipped school” to be true, one of the three nodes around it must be true. For “One of your professors runs into your parents and warns them” to be true, one of the two nodes below it must be true. In other words, if you can trace a path from an outermost node to the root node where all the nodes along the path are true, that means that the root node is true, and the attack is complete.

- “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 the table (8).

want to implement **Clandestinity (#3)** because you decide against going down that road.
- For the two “Targeted digital surveillance” techniques, **Digital best practices (#3)** is the only mitigation that makes sense in your context.

You update the 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 in the table. 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:

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 (#3)**.

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*

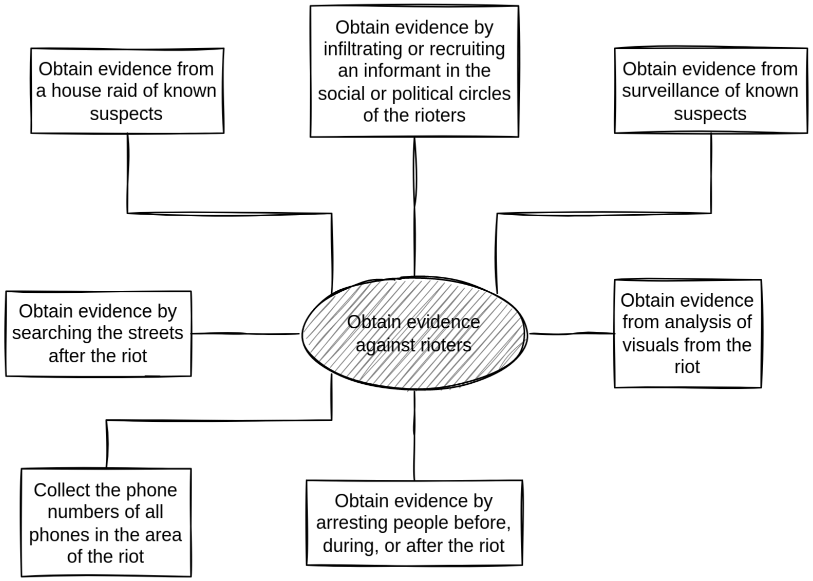
In this example, the adversary is the State and its cops, and their goal is to get enough evidence of your involvement in the riots to convince a judge to convict you. You draw an attack tree to represent the ways they could achieve this goal[8]. You begin with the root node (2).

[8] 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).

Obtain evidence against rioters

(2) “Riot” attack tree (root node)

You then add the immediate nodes, next to the root node (3). At this stage, you should add anything you can think of, even if you're not sure it applies to your context. The tree can grow in all directions, to make it more compact.

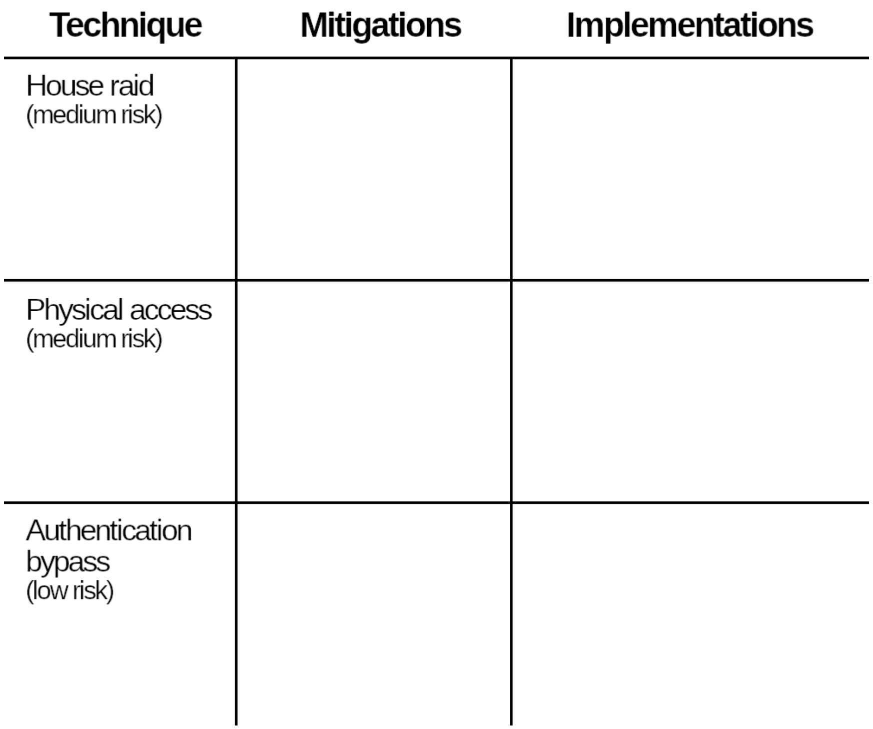

Obtain evidence from a house raid of known suspects
Obtain evidence by infiltrating or recruiting an informant in the social or political circles of the rioters
Obtain evidence from surveillance of known suspects
Obtain evidence by searching the streets after the riot
Obtain evidence against rioters
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

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

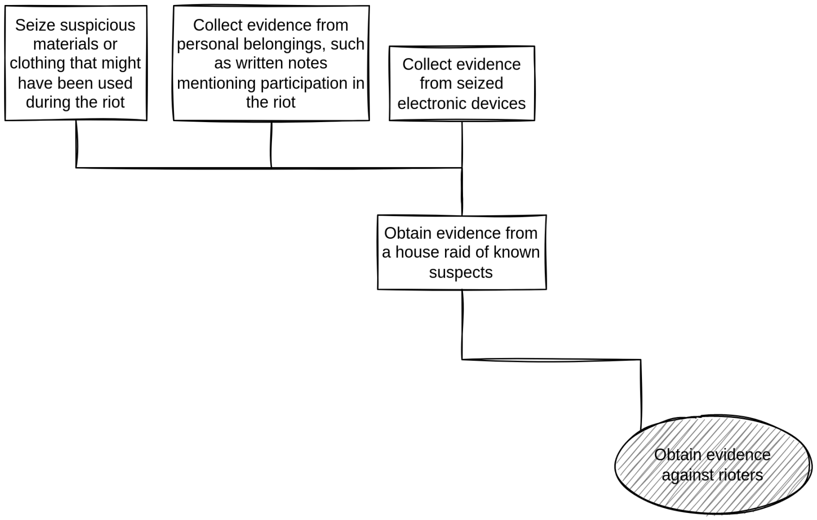
Next, you identify all the mitigations that you want to implement by looking at the mitigations that the Threat Library suggests for the techniques in the table.

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

- For “House raid”, **Preparing for repression (#3)**, **Preparing for house raids (#3)** and **Stash spot or safe house (#3)**. You don't

2.2.2. Identify techniques

You identify all techniques represented in the tree by matching 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

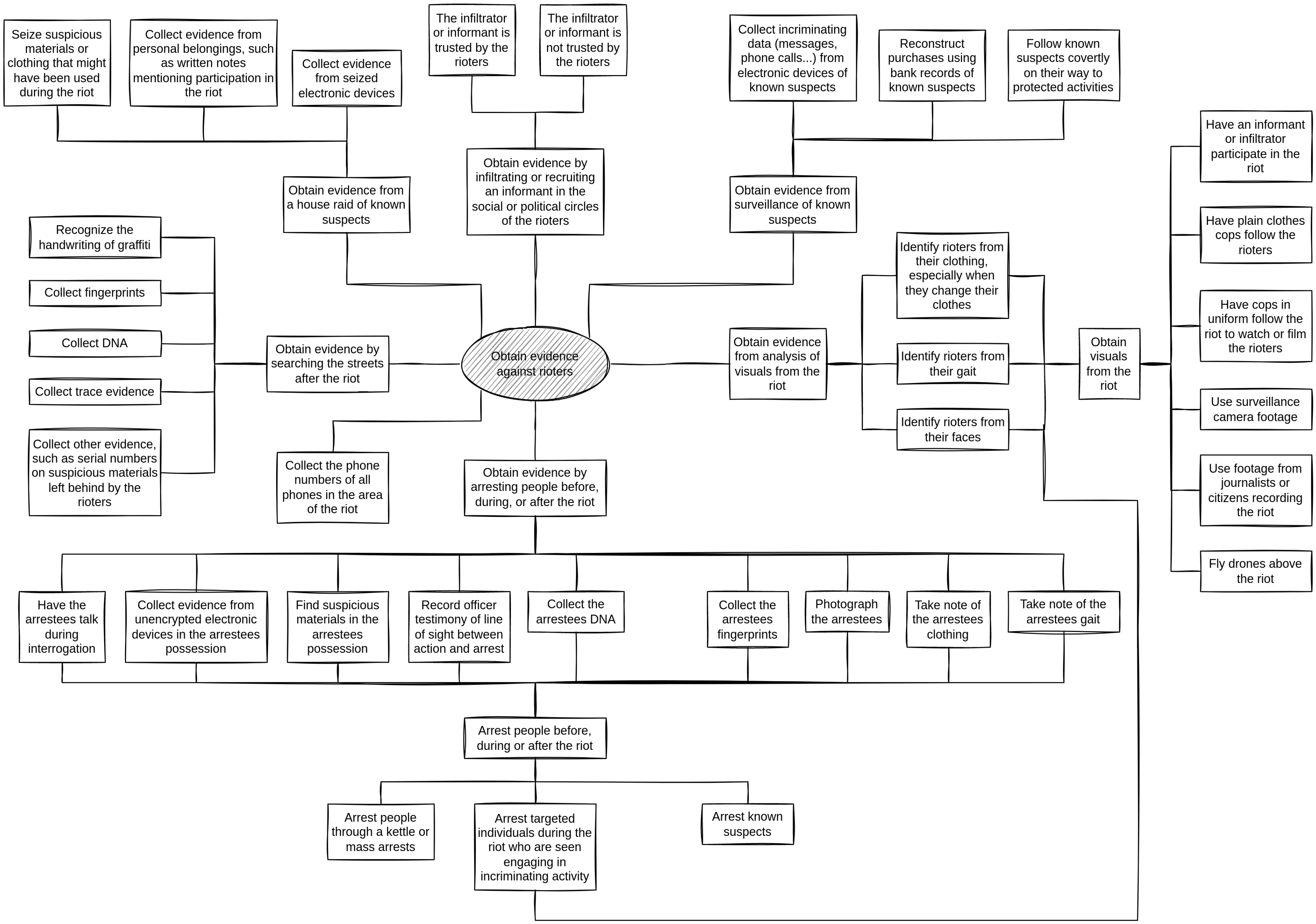
(5) “Riot” attack tree (house raid branch)

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 (#2)**.
- “Collect evidence from seized electronic devices” matches **Targeted digital surveillance: Physical access (#2)** because they would access your electronic devices, and **Targeted digital surveillance: Authentication bypass (#2)**, 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

takes practice. The tree is complete when no more nodes are needed to complete an attack, and every attack that you can think of is represented (4).


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
Have plain clothes cops follow the rioters
Recognize the handwriting of graffiti
Collect fingerprints
Collect DNA
Collect trace evidence
Collect other evidence, such as serial numbers on suspicious materials left behind by 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 clothing, especially when they change their clothes
Identify rioters from their gait
Identify rioters from their faces
Obtain visuals from the riot
Have cops in uniform follow the riot to watch or film the rioters
Use surveillance camera footage
Use footage from journalists or citizens recording the riot
Fly drones above 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
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, left part).

(4) “Riot” attack tree (complete, right part)