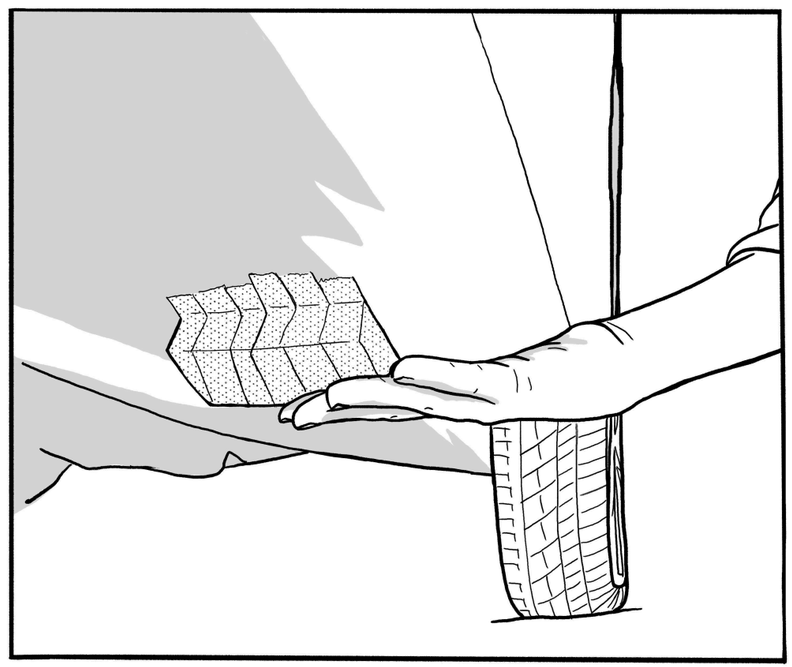
Threat Library

Part 1/2

Tutorial, Tactics, Techniques



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.

Digital best practices (#2): You can follow digital best practices to mitigate the risk of an adversary physically accessing your digital devices. For example, if you are going to an event or demonstration and you think that you could be arrested, you should not take your phone with you.

Network map exercise (#2): An adversary could physically access your digital devices through an **infiltrator (p. 31)** or **informant (p. 31)**. To mitigate this, you can conduct a network map exercise to help you decide who you trust to access your digital devices.

Physical intrusion detection (#2): You can use physical intrusion detection to detect when a space has been physically accessed by an adversary.

Tamper-evident preparation (#2): You can use tamper-evident preparation to detect when something has been physically accessed by an adversary.

Threat Library
Part 1/2: Tutorial, Tactics, Techniques
Part 2/2: 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

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. 40)**, by compromising your home router with **malware (p. 44)**, 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[72], 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 anarchist hacker Jeremy Hammond, in which the times when the alias he used in chat rooms was "online" (obtained through network traffic analysis[107]) were correlated with the times when a **physical surveillance (p. 37)** effort observed him at home to prove that the alias belonged to him.

Mitigations

Compartmentalization (#2): An adversary can establish links between different digital identities through the footprints left by their network traffic. To mitigate this, you can compartmentalize different digital identities by:

- Using Tails[9] and rebooting between each session.
- Using Qubes OS[108] with different Whonix[109] virtual machines that you use non-simultaneously.

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

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

[109] https://whonix.org

Digital best practices (#2): You can follow digital best practices, and in particular use Tor[72], to make it harder for an adversary to monitor and analyze your network traffic.

Encryption (#2): You can encrypt "in-motion" data to make it harder for an adversary to analyze the data with network forensics.

4.24.5. Physical access

Physical access is the process by which an adversary physically accesses an electronic device in order to read its data or compromise it.

Notable examples of electronic devices that an adversary can physically access include:

- Computers, phones, and storage devices (e.g. hard drives, USB sticks, SD cards).
- Printers, cameras, "smart" TVs.
- Vehicles. For example, navigation systems[110] in modern vehicles can store the location of the vehicle.

If an adversary physically accesses a device, they can:

- Read the device unencrypted data, or its encrypted data if it is turned on (and therefore its **encryption (#2)** is not effective).
- Compromise the device with **malware (p. 44)**.
- Compromise the device with a hardware keylogger[111].

An adversary can physically access a device:

- During a **house raid (p. 29)** or a **covert house search (p. 16)**.
- After arresting you if you have the device on you.
- During a border control.
- Through an **infiltrator (p. 31)** or **informant (p. 31)** that has access to the device.

Mitigations

Computer and mobile forensics (#2): You can use computer and mobile forensics to detect when a device has been physically accessed by an adversary.

[110] https://en.wikipedia.org/wiki/Automotive_navigation_system

[111] https://en.wikipedia.org/wiki/Hardware_keylogger

Contents

erator (which, in some contexts, may require a warrant).
- To record the activity of a target phone when the adversary knows where the phone is being used, but doesn't know its phone number.

See the IMSI-catchers topic[101].

Mitigations

Bug search (#2): You can conduct a bug search to detect the presence of an IMSI-catcher.

Detecting the presence of an IMSI-catcher can have several benefits:

- The 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 (#2): You can encrypt a phone "in-motion" data so that if the data is collected by an IMSI-catcher, it cannot be analyzed. For example, you can use end-to-end encrypted messaging applications instead of legacy texts and calls for your phone communications.

Repressive operations

Case against Boris (#2): Investigators used IMSI-catchers during **physical surveillance (p. 37)** 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[21].

4.24.3. Malware

Malware is malicious software installed on a digital device such as a computer, server, or mobile phone, to compromise the device. Malware can do many different things, but against anarchists and other rebels, it typically aims to gain visibility into the compromised device through remote screen capture and remote keylogging (recording the keys pressed on a keyboard), and to track the location of the device (in the case of phones).

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

Malware can be installed on a device:

- Remotely, typically through phishing[102] via email or text-based messages (SMS, etc.) To be effective, phishing often requires the target to open a malicious file or link.
- By **physical accessing (p. 45)** the device.

See the targeted malware topic[103].

Mitigations

Compartmentalization (#2): If an adversary installs malware on a Tails[9] USB stick or a Qubes OS[104] virtual machine that you use for different digital identities, they can tie the different identities together. To mitigate this, you can use different Tails USB sticks or Qubes OS virtual machines for different digital identities.

Computer and mobile forensics (#2): You can use computer and mobile forensics to detect traces of malware on a device on which malware is or was installed.

Digital best practices (#2): You can follow digital best practices, and in particular use security-oriented operating systems to make it harder for an adversary to install malware on your digital devices.

Encryption (#2): You can encrypt "in-motion" data to make it harder for an adversary to install malware through *network packet injection*, an installation vector for some forms of modern spyware, such as Pegasus[105].

Repressive operations

Scripta Manent (#2): Malware was installed on the computer of one of the accused comrades[106]. 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 (#2): Investigators made five requests to remotely install spyware[37]. Of these, one installation was successful (on an iPhone SE 2020) and provided access to a Signal group conversation.

[102] https://en.wikipedia.org/wiki/Phishing
[103] https://notrace.how/resources/#topic=targeted-malware
[104] https://www.qubes-os.org
[105] https://forbiddenstories.org/about-the-pegasus-project
[106] https://earsandeyes.noblogs.org/post/2019/01/27/more-precisions-keylogger-italy

partment of the German federal police was unable to decrypt after a year of effort[98].

- On phones, you can use GrapheneOS, whose FDE makes it difficult for an adversary to guess the encryption password by brute force: after 140 failed attempts, each is delayed for a full day[99].

Tamper-evident preparation (#2): You can use tamper-evident preparation to detect when a device has been **physically accessed (p. 45)**.

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.

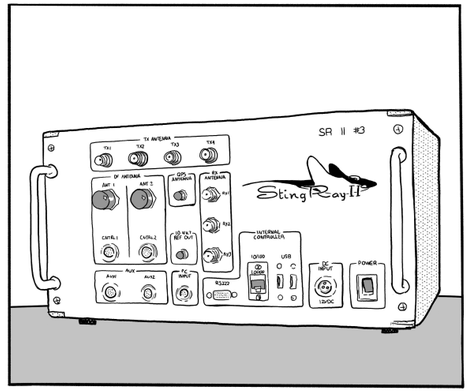
Repressive operations

Repression against Zündlumpen (#2): 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[100].

Repression of Lafarge factory sabotage (#2): Investigators recovered several encrypted smartphones in the raids and attempted to access their encrypted data, with varying results depending on the phone[37]:

- 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



An IMSI-catcher (also known as a *Stingray*) is an eavesdropping device used to collect information about all mobile phones that are turned on in a limited area (from a few meters to several hundred meters) around it. 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 legitimate cell towers.

An IMSI-catcher can collect the following information about the phones around it:

- Their numbers.
- Their IMSI numbers[90].
- Data and metadata about their activity: the content of SMS and regular calls, the list of visited websites, metadata about the use of end-to-end encrypted messaging applications (e.g. when Signal is used and the approximate size of messages sent or received through Signal).

An adversary can use an IMSI-catcher to link people and phone numbers. For example:

- At a public demonstration, to record the phone numbers of all the phones present at the demonstration and later obtain the names associated with those phone numbers through the **collaboration of the mobile network operators (p. 40)**.
- As part of a **physical surveillance (p. 37)** operation to record the target's phone number or the phone numbers of people the target meets with.

An adversary can also use an IMSI-catcher to record phone activity. For example:

- To record the activity of a target phone without requiring the collaboration of the mobile network op-

[97] https://debian.org

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

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

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

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:

- 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: participate in 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:

- The home page[5] provides an overview of all the tactics and techniques.
- The **techniques (p. 16)**, **mitigations (#2)**, and **repressive operations (#2)** 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] https://notrace.how/resources/#keimeno-ton-prophulakismenon-tes-neas-philadelpheias

[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

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

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.

Case against Boris (#2): With the collaboration of mobile network operators, investigators intercepted calls from Boris's phone or the phones of people close to him[21]. They regularly listened to the intercepted calls in real time and used information from the calls to adjust ongoing **physical surveillance (p. 37)** 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 (#2): 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 investigators with the collaboration of the bank[34].

Repression of Lafarge factory sabotage (#2): Investigators gave the serial number of a camera to the camera manufacturer, and the manufacturer gave them the name of the store where the camera was sold[37]. This helped investigators identify a person they accused of taking photos with the camera.

Prometeo (#2): Investigators distorted conversations obtained through phone interception to make them look suspicious[77]. 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 (#2): 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[39].

4.24. Targeted digital surveillance

Used in tactics: **Incrimination (p. 15)**

Targeted digital surveillance is the targeted collection and analysis of digital data and communications.

Extremely advanced techniques exist[96] in the arsenal of nation-State actors, but the focus here is on techniques that are more likely to be used against anarchists and other rebels.

See the digital surveillance topic[71].

4.24.1. Authentication bypass

Authentication bypass is the process by which an adversary bypasses the **Full Disk Encryption (#2)** that protects access to a digital device. An adversary can achieve authentication bypass through human error, weak passwords, or technical exploits.

An adversary can achieve authentication bypass through:

- Accessing the device while it is turned on (and therefore its encryption is not effective).
- Finding the encryption password written down somewhere.
- Making the device owner provide the encryption password by using **interrogation techniques (p. 32)** including, in some contexts, **extra-legal violence (p. 21)**.
- Visual interception: watching the device owner type the encryption password through a **hidden camera (p. 19)** or an **infiltrator (p. 31)**.
- Brute force: guessing the password through repeated, automated authentication attempts.
- Compromising the device either through remotely-installed **malware (p. 44)** or **physical access (p. 45)**.
- Exploiting a flaw at the implementation level of the encryption process.

Mitigations

Bug search (#2): Before entering a password in a room where **covert video surveillance devices (p. 19)** may be present, you can conduct a bug search to locate such devices and eventually remove them.

Digital best practices (#2): You can follow digital best practices, and in particular use security-oriented operating systems with Full Disk Encryption (FDE) and strong passwords, to make it harder for an adversary to bypass authentication on your digital devices. For example:

- On computers, you can use the Linux FDE called LUKS, which is used by many Linux systems, such as Debian[97] and Tails[9], and which the forensics de-

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

- If you follow **digital best practices (#2)** 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

Mobile network operators can provide:

- Given a name: the phone numbers registered under that name.
- Given a phone number: the name under which the phone number is registered and the IMSI number[90] of the phone in which the phone number is used.
- Given an IMSI number: the phone number that is used in the phone with that IMSI number.

Additionally, given your phone number, mobile network operators can provide (current and historical) data and metadata about your phone activity:

- The content of SMS and regular calls you make on your phone.
- The list of websites you visit on your phone.
- Your phone physical location.
- Metadata about your use of end-to-end encrypted messaging applications (e.g. when you use Signal and the approximate size of messages sent or received through Signal).

This means that any of the following conditions allows the State to access (current and historical) data and metadata about your phone activity:

- Knowing your name (if your phone is not **anonymous (#2)**).
- Knowing your phone number, which they can find by monitoring or seizing a phone in contact with yours, using an **IMSI-catcher (p. 43)**, or through advanced correlation techniques[91].
- Knowing your phone IMSI number, which they can find by seizing your phone.

[90] An International Mobile Subscriber Identity (IMSI) number is a number that uniquely identifies a phone, and that is sent from the phone to the mobile network operator when the phone connects to the network.

[91] For example, if the State 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, they can deduce the phone is yours.

Online services

Websites, email providers, and other online services can provide:

- The content of unencrypted communications you make through the service (e.g. social media posts, unencrypted emails).
- Metadata about encrypted communications you make through the service (e.g. the sender, recipient, and date of encrypted emails).

Mitigations

Anonymous phones (#2): You can use anonymous phones to make it harder for an adversary to use the collaboration of mobile network operators to establish links between your identity and the phones you use.

Anonymous purchases (#2): If you need to purchase an item in a store, you can purchase it anonymously to make it harder for an adversary to use the collaboration of the store to link your identity to the item.

Digital best practices (#2): You can follow digital best practices to make it harder for an adversary to use the collaboration of service providers to obtain information about you. For example, you can:

- Use Tor[72] so that an adversary cannot obtain data about your Internet activity through the collaboration of your Internet service provider.
- Use trusted online services[92] that 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.
- Use peer-to-peer applications such as Cwtch[93] and Briar[94] for communication or OnionShare[95] for file sharing to avoid having to trust a service provider.

Encryption (#2): You can encrypt "in-motion" data to limit the ability of untrusted service providers to collaborate with an adversary.

Repressive operations

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

[93] https://cwtch.im

[94] https://briarproject.org

[95] https://onionshare.org

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].

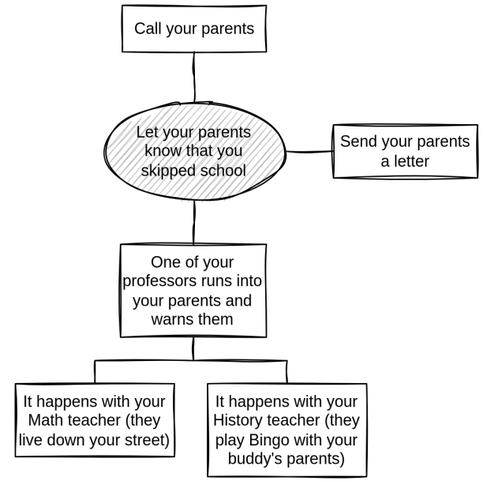
Attack trees are a tool to facilitate a brainstorming exercise on the different ways an adversary could successfully attack you in a given context by representing the attacks —the threats—in a tree structure. They help understand how a plan or project is vulnerable to repression by modeling the options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



(1) "Skipping school" attack tree

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.

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 (#2)**.

[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

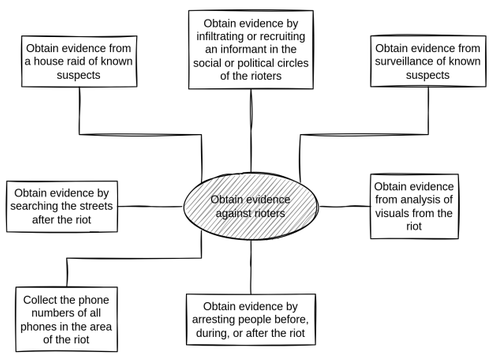
The goal of the discussion: draw an attack tree, identify techniques and mitigations that apply to your context, and decide how to implement those mitigations. After the riot, it may be a good idea to conduct an *action review*.

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).

(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. You can grow the tree in all directions, to make it more compact.



(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 nodes are needed to complete an attack, and every attack that you can think of is represented (4).

[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).

- Foot movement.
- **Helicopters, drones or surveillance planes (p. 37)**.

Routine patrols

Routine police patrols usually occur in extended perimeters around police stations. They serve to establish a visible police presence to deter potential criminals, and occasionally to catch unlucky criminals "red handed".

Patrols in response to a threat

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. 28)** or **civilians (p. 33)**.
- An **alarm system (p. 16)** (e.g. motion detectors inside a building), either directly or through a security company monitoring the alarm system.
- Police officers monitoring live **CCTV footage (p. 34)**.
- An **infiltrator (p. 31)** or an **informant (p. 31)**.

Mitigations

Attack (#2): The police can disturb an action. To mitigate this, you can distract them 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.

The police can follow you after an action. To mitigate this, you can use tactics designed to stop them or slow them down, either preventively or during the pursuit: crow's feet or spike strips, gunfire, barricades, stones, fireworks, etc.

Careful action planning (#2): You can carefully plan an action to take into account the risk of routine police patrols interfering with the action, a risk that is always present, except perhaps in remote areas.

Reconnaissance (#2): Before an action, you can identify the nearest police station, their shift change schedule, and patrol patterns, and 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. 15)**

Service provider collaboration is the process by which an entity that has information about you because it provides a service to you is asked or legally compelled to provide that information to the State. Service provider collaboration can provide both current and historical information, and can occur both retrospectively and in real time.

State institutions

State institutions such as social services and hospitals can provide any information they have about you, including your address, marital status, social benefits, health information, etc.

Stores

Physical and digital stores can provide information about purchases made through the store, including:

- Given a name: the items purchased under that name, as well as the date of the purchases.
- Given an item or category of items: the names of the people who purchased the item, as well as the date of the purchases.

Additionally, physical stores can provide:

- CCTV footage from cameras operated by the store.
- Testimony from store employees, for example about the physical appearance of a person who made a particular purchase.

Banks

Banks can provide:

- Your bank account activity, including the date, location and amount of any purchase or withdrawal you make with a card.
- CCTV footage from cameras on ATMs.

Internet service providers

Internet service providers can provide:

Transportation by bike (#2): You can use a bike instead of any other type of vehicle: compared to other vehicles or people on foot, a bike is harder to follow by a mobile physical surveillance effort, especially without the effort being detected.

Repressive operations

Case against Boris (#2): For several weeks, investigators regularly staked out Boris's home and tailed him as he moved on foot, on bicycles, and in vehicles[21].

Repression of the first Jane's Revenge arson (#2): In March 2023, cops secretely observed the comrade who was later arrested from a distance of about 30 meters[40]. The cops watched the comrade discard a paper bag, retrieved it, and collected DNA evidence linking the comrade to the action site.

Case against Jeff Luers (#2): 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[55]. 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 (#2): 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[78]. 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.

Nea Filadelphia case (#2): On the day of the arrests, when one of the comrades visited a cybercafé that was probably under police surveillance, cops recognized him and started following him[88]. 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[89]—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. 36)** 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 (#2): You can dress anonymously at a demonstration or other event to make it harder for an overt surveillance effort to identify you.

Repressive operations

Mauvaises intentions (#2): 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[39].

4.22. Police patrols

Used in tactics: **Arrest (p. 15)**, **Deterrence (p. 15)**, **Incrimination (p. 15)**

Police patrols are the law enforcement practice of traversing a particular area to monitor and secure it. Police may conduct patrols either as a routine operation or in response to a perceived threat in an area.

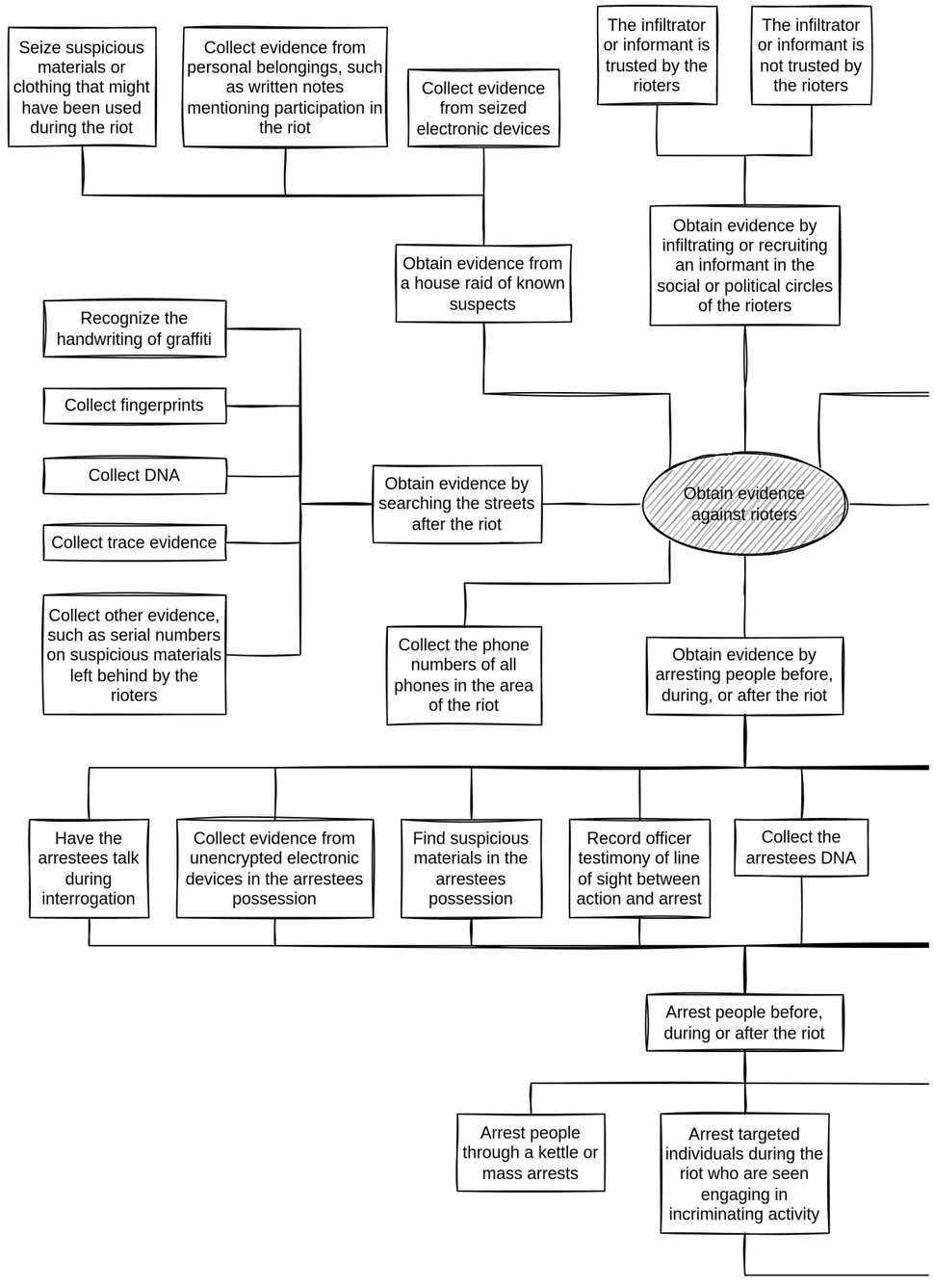
Means of transportation

Police patrols can use different means of transportation:

- Marked or unmarked vehicles.

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

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



(4) "Riot" attack tree (complete, left part).

Attack (#2): 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[83].

Surveillance detection (#2): You can conduct surveillance detection to detect most and helicopters and some drones by listening for potential helicopters and drones: you should be able to hear most of them, depending on their altitude and your surroundings.

Repressive operations

Berlin 2023 railway conspiracy case (#2): The arrested comrades were discovered at night by a helicopter on a routine surveillance flight, presumably equipped with night-vision equipment[84]. A text[85] 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 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 (#2): Drones were used to track rioters leaving riots in order to facilitate their arrest[29].

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. 18)** installed on the target's vehicle or bike.
- **Aerial surveillance (p. 37)**, such as a drone following the target from a distance.

Generally, a surveillance team will not attempt to arrest its target during a mobile physical surveillance operation. On rare occasions, however, this may happen if the surveillance team has gathered enough information about the target's activities to incriminate them and deems it necessary to arrest the target immediately (e.g. to prevent a crime).

See also:

- Measures Against Surveillance[86] for insights into how police and intelligence agencies conduct such surveillance and how we can defend against it.
- The physical surveillance topic[87].

Mitigations

Anti-surveillance (#2): You can conduct anti-surveillance to evade a mobile physical surveillance effort.

Surveillance detection (#2): You can conduct surveillance detection to detect a mobile physical surveillance effort.

[83] https://notrace.how/resources/#cinq-manieres-a-la-portee-de-tous-pour-abattre-un-drone
[84] https://notrace.how/resources/#wir-haben-eine-verabredung
[85] https://kontrapolis.info/9821
[86] https://notrace.how/resources/#massnahmen-gegen-observation
[87] https://notrace.how/resources/#topic=physical-surveillance

2019-2020 case against Mónica and Francisco (#2): The photos used to identify Mónica and Francisco in public CCTV footage were found on social media[33].

Repression of Lafarge factory sabotage (#2): Investigators collected metadata from photos of the action posted online, including the name and serial number of a camera[37]. This helped them identify a person they accused of taking the photos.

4.20. Parallel construction

Used in tactics: **Incrimination (p. 15)**

Parallel construction is the unlawful 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 can collect incriminating digital evidence from a phone without a warrant, and then conduct a **house raid (p. 29)** to seize the phone where that evidence can be "discovered" so that it will not be 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. 15)**

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. 39)** surveillance effort.
- Improving the chances of successfully following the target of surveillance during a **mobile physical surveillance (p. 38)** 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[79]).
- Locating suspects as part of routine **police patrols (p. 39)** 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[80], with high-quality video at night[81].

See the aerial surveillance topic[82].

Mitigations

Anonymous dress (#2): 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).

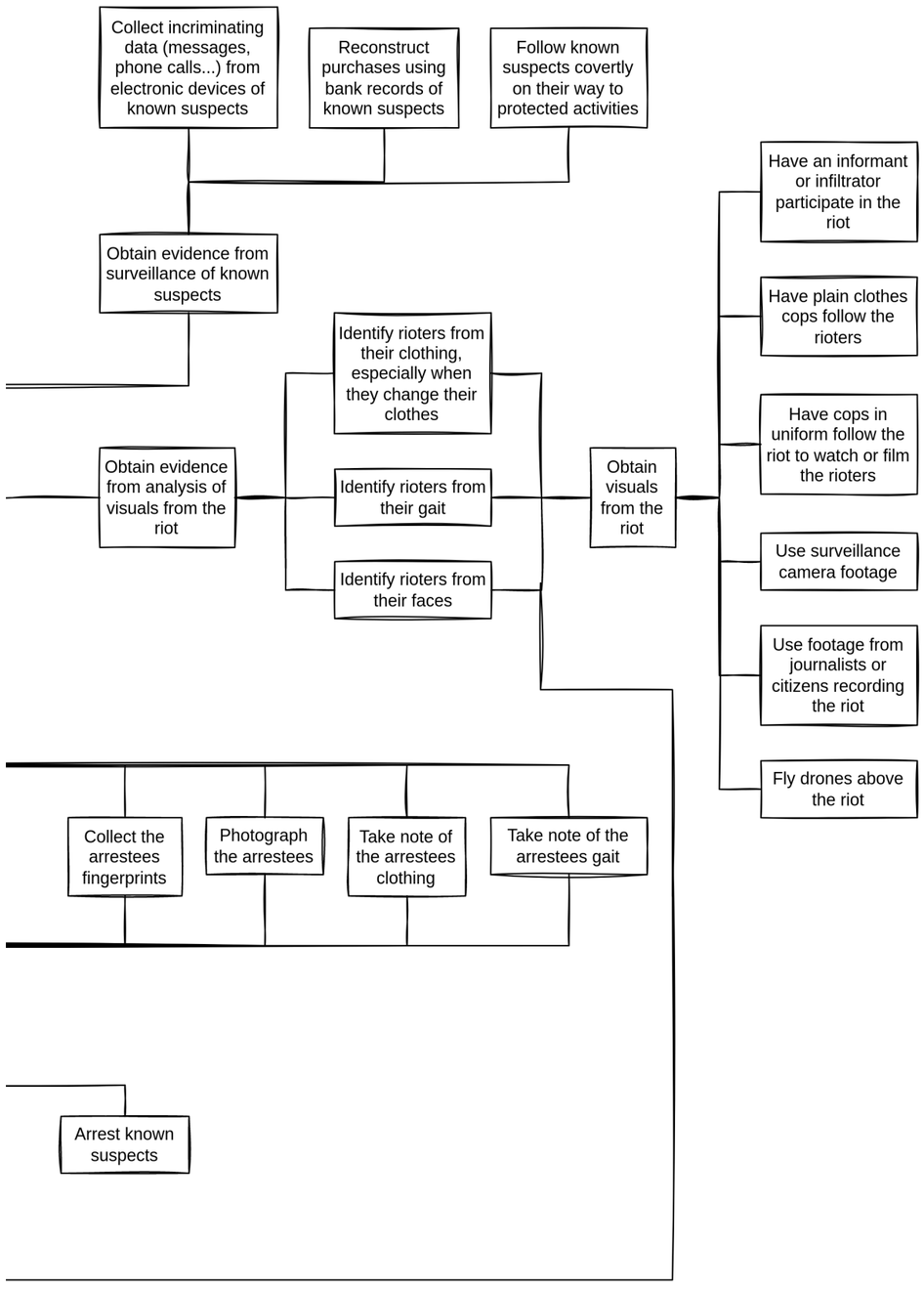
Anti-surveillance (#2): You can include in an anti-surveillance route locations that would prevent an aerial surveillance effort from following you: an underground metro system, a shopping complex with many entrances, etc.

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

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

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

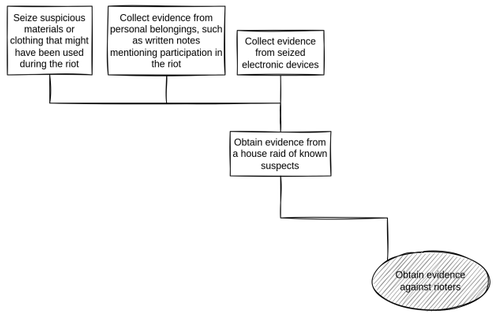
[82] https://notrace.how/resources/#topic=aerial-surveillance



(4) "Riot" attack tree (complete, right part)

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.



(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. 29)**.
- "Collect evidence from seized electronic devices" matches **Targeted digital surveillance: Physical access (p. 45)** because they would access your electronic devices, and **Targeted digital surveillance: Authentication bypass (p. 42)**, 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 section "Assessing Risk", p. 13 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 (#2)**, **Preparing for house raids (#2)** and **Stash spot or safe house (#2)**. You don't want to implement **Clandestinity (#2)** because you decide against going down that road.
- For the two "Targeted digital surveillance" techniques, **Digital best practices (#2)** is the only mitigation that makes sense in your context.

You update the table (7).

Repression of the first Jane's Revenge arson (#2): 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[40].

The three from the park bench (#2): 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 video surveillance cameras buying gas and filling a gas can[78]. The cops got the CCTV footage the next morning.

4.18. Network mapping

Used in tactics: **Incrimination (p. 15)**

Network mapping is the process by which an adversary gains insight into the organization and social relationships of a given network. By gaining this insight, an adversary can select individuals for additional scrutiny, arrest, or recruitment as **informants (p. 31)**.

The State very frequently uses social media friends lists (a form of **open-source intelligence (p. 36)**) for network mapping because they do not require a warrant or legal authorization.

Mitigations

Anonymous phones (#2): You can use anonymous phones to make it harder for an adversary to conduct network mapping.

Avoiding self-incrimination (#2): An adversary can use information obtained through self-incrimination to endanger not only the individual from whom the information was obtained, but also the rest of their network. To mitigate this, you should not talk to an adversary under any circumstances, and you can avoid providing biometric information (face photograph, fingerprints, DNA) if possible.

Compartmentalization (#2): You can compartmentalize your different identities (or projects) to make it harder for an adversary to conduct network mapping.

Digital best practices (#2): You can follow digital best practices, and in particular use end-to-end encrypted messaging applications on encrypted devices, to obscure your social networks and make it harder for an adversary to conduct network mapping.

Fake ID (#2): During an ID check, you can present a fake ID to make it harder for the State to conduct network mapping.

Need-to-know principle (#2): You can apply the need-to-know principle to make it harder for an adversary to conduct network mapping.

Network map exercise (#2): An adversary can conduct network mapping by using infiltrators and informants to monitor networks: infiltrators and informants build credentials through association, build social profiles of people in the network, find pressure points to instigate interpersonal and political conflict, and entrap people. To mitigate this, you can conduct a network map exercise to make your network more resilient to infiltration attempts and help ensure it does not place trust in people who could become informants.

Repressive operations

Mauvaises intentions (#2): To prove that the accused comrades knew each other and were therefore likely accomplices, the investigators used several clues[39]:

- 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

4.19. Open-source intelligence

Used in tactics: **Incrimination (p. 15)**

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 (#2): An adversary can use open-source intelligence to collect information that you publish voluntarily. To mitigate this, you can avoid using social media and generally avoid making any information about yourself or your networks public.

Repressive operations

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

- Retroactively if the CCTV footage has been stored. Retroactive analysis can help identify a suspect by their **face (p. 25)**, **gait (p. 26)**, **voice (p. 27)**, etc.

Analysis of CCTV footage can be performed:

- By humans.
- By automated systems such as automated license plate readers or **facial recognition systems (p. 25)**.

See also

- You Can't Catch What You Can't See: Against Video Surveillance[73].
- The topics video surveillance[74] and automated license plate readers[75].

Mitigations

Anonymous dress (#2): You can dress anonymously to prevent an adversary from identifying you from CCTV footage.

Anonymous purchases (#2): You can make anonymous purchases to prevent an adversary from identifying you from CCTV footage of physical stores.

Attack (#2): You can disable[76] surveillance cameras.

Biometric concealment (#2): When filmed by surveillance cameras, you can:

- To prevent **gait recognition (p. 26)**, wear baggy clothing that hide your body shape, use an umbrella or other concealing objects, or drastically change your walking style by adopting a "funny walk".
- To prevent **facial recognition (p. 25)**, 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 (#2): You can conduct sensitive conversations away from surveillance cameras to prevent an adversary from recording those conversations with surveillance cameras equipped with microphones.

Reconnaissance (#2): Before an action, you can identify the location of surveillance cameras at an action site and make plans to avoid them if possible.

Transportation by bike (#2): You can use a bike instead of any other type of vehicle: compared to other vehicles, a bike is much harder to identify on CCTV footage, especially if its distinguishing features are minimized. For example, you can use a different stolen bike for each action you carry out.

Repressive operations

Case against Boris (#2): 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[21].

2019-2020 case against Mónica and Francisco (#2): Public CCTV footage was extensively used by investigators to reconstruct the movements of Mónica and Francisco before and during the actions, despite the mitigations they took (taking taxis, changing clothes, wearing disguises)[33].

Repression of Lafarge factory sabotage (#2): 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[37]. In particular, footage of the interiors of buses appears to have helped identify people traveling to and from the action site[36]. 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 (#2): Two of the accused comrades were allegedly seen on a video surveillance camera leaving a store where investigators believe the envelopes used to prepare the parcel bombs were purchased[77].

2013 case against Mónica and Francisco (#2): Public CCTV footage was used by investigators to reconstruct the movements of Mónica and Francisco before and after the action[45]. This showed that they were near the action site shortly before the explosion of the device.

[73] https://notrace.how/resources/#pas-vue-pas-prise
[74] https://notrace.how/resources/#topic=video-surveillance
[75] https://notrace.how/resources/#topic=automated-license-plate-readers
[76] https://notrace.how/resources/#detruisons-les-cameras
[77] https://ilrovescio.info/2020/08/23/uno-scritto-di-natascia-dal-carcere-di-piacenza

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:

- "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).

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 works when turned on and locked?
Authentication bypass (low risk)	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 (#2)**). 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. Conduct an action review

After the riot, you and your comrades take some time to conduct an action review: in **outdoor and device-free conversations (#2)**, you discuss what went well and what went wrong, and whether there is room for improvement

[9] https://tails.net

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 (p. 23)** 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.
- 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 (#2)** 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 (#2)** 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.

to facilitate the work of law enforcement and intelligence agencies worldwide.

See the digital surveillance topic[71].

Mitigations

Avoiding self-incrimination (#2): An adversary can use mass digital surveillance to retrieve self-incriminating information from a digital device. To mitigate this, you can avoid storing such information on digital devices except for very deliberate reasons (such as writing and sending an action claim while following **digital best practices (#2)**).

Digital best practices (#2): You can follow digital best practices to make mass digital surveillance ineffective. For example, you can use Tor[72] to anonymize your Internet activity, and you can use security-oriented operating systems and applications that limit the data they store or collect about you.

Encryption (#2): You can encrypt "in-motion" data to prevent observers at certain points on the network from analyzing this data.

4.17.3. Police files

Police files are physical or digital records maintained by law enforcement agencies. Police files contain vast amounts 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.

Notable 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. 30)**, fines, arrests, investigation proceedings, judicial proceedings, and convictions.

Mitigations

Attack (#2): You can destroy cabinets that store police files on paper and data centers that store them digitally.

Repressive operations

Case against Boris (#2): Investigators found out that the DNA on the bottle cap belonged to Boris because his DNA was in France's national DNA database[21].

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

Mass video surveillance (also known as *close-circuit television*, or *CCTV*) is the large-scale collection, storage and analysis of video and audio data from video surveillance cameras. Mass video surveillance aims to capture the identity of people who pass through a space and to extend its coverage to as much space as possible. Some countries now have more surveillance cameras than citizens.

Collection

Sources of CCTV footage include:

- Cameras in the street or in other public locations.
- Cameras in private buildings (e.g. shops, offices).
- Public transport cameras on buses, trains, highways, etc.
- Home surveillance systems such as Amazon Ring.
- In-vehicle surveillance systems like those found on Teslas.

CCTV cameras can vary widely in quality, range, night vision capabilities, presence of microphones, etc.

Storage

After its collection, CCTV footage is often stored for some time (from weeks to indefinite durations) before being erased.

Analysis

An adversary can analyze CCTV footage:

- In real time if the cameras are integrated into a central network. Real-time analysis can take place either as part of routine police surveillance or during exceptional events (e.g. demonstrations).

[71] https://notrace.how/resources/#topic=digital-surveillance
[72] https://torproject.org

For a comprehensive overview of interrogation techniques and how to resist them, see How the police interrogate and how to defend against it[70] (in French and German).

Mitigations

Avoiding self-incrimination (#2): 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 (#2): When interrogating people close to Boris, investigators used elaborate lies to try to get information from them[21]. 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?"

4.17. Mass surveillance

Used in tactics: **Deterrence (p. 15)**, **Incrimination (p. 15)**

Mass surveillance is the large-scale surveillance of an entire or substantial portion of a population. It is the surveillance baseline of our society.

4.17.1. Civilian snitches

Civilian snitches are people who are not part of an adversary's security force, but who would inform the adversary if they saw something suspicious.

For example, a civilian snitch 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 the suspects until the police intervene or become a witness in a criminal investigation.

Mitigations

Anonymous dress (#2): You can dress anonymously to prevent civilians from providing a description of you that would be valuable to an adversary.

Attack (#2): If a civilian follows you after an action, you can scare them off with threats or pepper spray. If a civilian tries to call the police, you can destroy their phone.

Careful action planning (#2): Civilians can observe you during actions and report their observations to an adversary. To mitigate this, you can carry out actions at night or in areas with minimal foot traffic to minimize witnesses, and use a lookout to report the presence of any witnesses as soon as they are noticed. Beware of balconies and windows overlooking the scene.

Repressive operations

2019-2020 case against Mónica and Francisco (#2): The saleswoman of the cell phone store where Mónica bought a phone that was used as part of the 2020 action, when questioned by investigators, gave a description of a person that the investigators matched to Mónica[33].

Belarusian anarcho-partisans (#2): 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.

4.17.2. Mass digital surveillance

The Utah Data Center (UDC), a giant data storage facility in Utah, United States, used for mass digital surveillance purposes by U.S. intelligence agencies.

Mass digital surveillance is the large-scale collection, storage, and analysis of the digital communications of an entire or substantial portion of a population.

Mass digital surveillance relies on the collection of data from a variety of sources: financial transactions, border controls, GPS tracking of smartphones, and even "smart" streetlights. Technological advances in storage capacity allow vast amounts of data to be stored in State-controlled data storage facilities. Technological advances in processing power enable automated analysis of this data

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

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 (#2)** for more information.

3. Tactics

3.1. Deterrence

Uses techniques:

Door knocks (p. 20)
Extra-legal violence (p. 21)
Increased police presence (p. 30)
Mass surveillance (p. 33)
Police patrols (p. 39)

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 (p. 16)
Covert surveillance devices (p. 17)
Detection dogs (p. 20)
Door knocks (p. 20)
Evidence fabrication (p. 21)
Extra-legal violence (p. 21)
Forensics (p. 22)
House raid (p. 29)
ID checks (p. 30)
Infiltrators (p. 31)
Informants (p. 31)
International cooperation (p. 32)
Interrogation techniques (p. 32)
Mass surveillance (p. 33)
Network mapping (p. 36)
Open-source intelligence (p. 36)
Parallel construction (p. 37)
Physical surveillance (p. 37)
Police patrols (p. 39)
Service provider collaboration (p. 40)
Targeted digital surveillance (p. 42)

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. 16)
Detection dogs (p. 20)
Guards (p. 28)
House raid (p. 29)
ID checks (p. 30)
Increased police presence (p. 30)
International cooperation (p. 32)
Police patrols (p. 39)

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

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 of their cooperation, people who are no longer in a network and harbor feelings of resentment, people who prioritize money over dignity, etc.

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

See the informants topic[63].

Mitigations

Attack (#2): You can attack informants when uncovered or years later to discourage others from becoming informants.

Background checks (#2): You can perform background checks to help ensure that someone in your network is not an informant.

Need-to-know principle (#2): You can apply the need-to-know principle to limit the information a potential informant has about your involvement in actions (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 (#2): You can conduct a network map exercise to help ensure your network does not place trust in people who could become informants.

Prisoner support (#2): You can support prisoners from your networks: beyond the ethical imperative of this support, 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 (#2): 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[65]. Frank Ambrose became an informant after his arrest in 2007 (which was triggered by him throwing incriminating material in a garbage can)[66]. 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[67].

4.15. International cooperation

Used in tactics: **Arrest (p. 15)**, **Incrimination (p. 15)**

International cooperation is the exchange of information between law enforcement and intelligence agencies of different countries.

International cooperation can be used to:

- Exchange intelligence.
- Facilitate the incrimination, arrest and deportation of suspects across national borders.

International cooperation can happen through informal channels, or through formal organizations such as Interpol.

Repressive operations

Bialystok (#2): In June 2020, comrades were arrested in Spain and France, thanks to cooperation between Italian, Spanish and French intelligence and police forces[68]. During the investigation Italian cops tried to target a person living in Germany[69]. They sent several requests to German police to extradite the person or have their house searched but the requests were rejected.

Scintilla (#2): Carla was arrested in France thanks to cooperation between Italian and French intelligence and police forces[49].

4.16. Interrogation techniques

Used in tactics: **Incrimination (p. 15)**

Interrogation techniques are the methods used by an adversary to obtain information from suspects during interrogations.

Interrogation techniques can include lying, making threats, instilling guilt, shame, or pride, trying to appear friendly and helpful or, on the contrary, threatening and violent, etc. In some cases, they can include **extra-legal violence (p. 21)**.

[65] https://supportmariusmason.org/about-marius/about-the-case
[66] https://www.mlive.com/news/ann-arbor/2008/10/activist_turned_informant_sent.html
[67] https://animalliberationpressoffice.org/NAALPO/snitches
[68] https://malacoda.noblogs.org/anarchici-imprigionati
[69] https://attaque.noblogs.org/post/2022/02/20/italie-allemagne-de-rome-a-bialystok-en-passant-par-berlin

tralized 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[61].

Careful action planning (#2): You can carefully plan an action to mitigate the risk of an increased police presence at the action site. For example:

- You can conduct a thorough **reconnaissance (#2)** of the action site and prepare a good escape plan.
- If you are planning to carry out arson, you can use an incendiary device with a delay so that the device is not activated until after you have left the action site.
- You can take advantage of the fact that an increased police presence in one place means the possibility of a decreased police presence elsewhere.

4.13. Infiltrators

Used in tactics: **Incrimination (p. 15)**

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[62] 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.

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

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

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[63].

Mitigations

Attack (#2): You can attack infiltrators when uncovered or years later[64] to discourage the practice—police infiltrators are likely to be less enthusiastic if there is a local precedent of violence against them.

Background checks (#2): You can perform background checks to help ensure that someone in your network is not an infiltrator.

Need-to-know principle (#2): You can apply the need-to-know principle to limit the information a potential infiltrator has about your involvement in actions (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 (#2): You can conduct a network map exercise to make your network more resilient to infiltration attempts.

4.14. Informants

Used in tactics: **Incrimination (p. 15)**

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

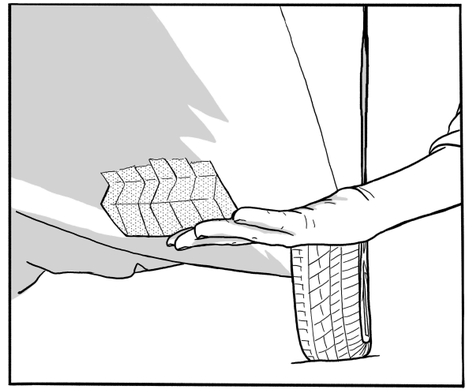
An informant can be used by an adversary to find evidence or to achieve **network mapping (p. 36)**.

There are several different recruitment strategies: targeting people on the periphery of a network who are less

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

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

4. Techniques



4.1. Alarm systems

Used in tactics: **Arrest (p. 15)**

Alarm systems are mechanisms that protect physical or digital infrastructure by sending an alert signal when unauthorized access to the infrastructure is detected. The alert signal can lead to the rapid intervention of security guards or law enforcement in order to investigate the situation.

For physical infrastructure, modern alarm systems typically include sensors that detect unauthorized access to an area outside of normal operating hours. Such sensors include infrared motion detectors, sensors that detect the opening of doors, and many other types of sensors[10]. 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[11] monitor for any activity that might indicate a hack is in progress. If unauthorized access is detected, an incident response team can be notified to attempt to contain and remediate any compromise.

Mitigations

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

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

Attack (#2): You can attack alarm systems or the communication lines they use to send alert signals. For example, you can destroy alarm systems or jam alert signals with a jamming device.

Some alarm systems operate by sending signals periodically or continuously, even when nothing abnormal is detected. In such cases, if you attack an alarm system in such a way that its signals are interrupted, this may be interpreted as an alert and trigger an intervention.

Digital best practices (#2): When carrying out a cyber action, you can use digital evasion techniques[12] to prevent intrusion detection systems from detecting the action.

Reconnaissance (#2): 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. Covert house search

Used in tactics: **Incrimination (p. 15)**

A covert house search is a discreet search of a residence conducted by an adversary when the occupants are not present.

An adversary can conduct a covert house search to:

- Gather information.
- Install **covert surveillance devices (p. 17)** in the residence.
- Install **malware (p. 44)** on digital devices.

Generally, when an adversary conducts a covert house search of a residence, they do not want the occupants to know that the operation has taken place. Therefore, in general:

- If the residence has locked doors, the adversary must bypass the doors without visibly breaking them. They can do this by picking the locks or asking the building owner for the keys.
- The adversary refrains from seizing items or moving things.

In addition to searching the residence, the adversary can covertly seize garbage from outside the residence in the

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

hope of finding valuable information (e.g., written notes, forensics evidence such as DNA traces).

Mitigations

Clandestinity (#2): If you enter clandestinity, an adversary cannot know where you live, and therefore cannot conduct a covert house search of your home.

Physical intrusion detection (#2): You can use physical intrusion detection to detect a covert house search.

Preparing for house raids (#2): 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 (#2): You can keep action materials that have no "legitimate" purpose in a stash spot or safe house, or at worst, let them pass through your home only for a very limited time.

4.3. Covert surveillance devices

Used in tactics: **Incrimination (p. 15)**

Covert surveillance devices are electronic devices hidden by an adversary to collect data: audio, video, and location data.

Where

An adversary can hide covert surveillance devices in buildings, in or on vehicles, or outdoors. Notable locations include:

- Microphones and cameras hidden inside the home of a target.
- Location trackers hidden in or on the vehicle of a target.
- Cameras hidden at the windows of a building close to the home of a target, such that the cameras can film the entrance to the home.

When

An adversary can hide covert surveillance devices for long-term surveillance (e.g. weeks, months or years), or short-term surveillance of specific events. A covert surveillance device can disappear:

- Most often, when it is retrieved by its installers.
- In some cases, when it is inadvertently discovered and removed by a third party.
- In rare cases, when it is deliberately discovered (through a **bug search (#2)**) and removed by a third party.

Power supply

Covert surveillance devices require a power supply, which can be either a battery or the electrical system of the building or vehicle in which the device is hidden, or both. In rare cases, they may be powered by Power over Ethernet (PoE). To save battery power and make it harder to detect them, devices may not be powered on all the time.

Data transmission

Covert surveillance devices often transmit the data they collect:

- Most often for low-cost modern devices, over the mobile phone network using a SIM card included in the device.
- In some cases over WiFi, Bluetooth, Ethernet, or arbitrary radio frequencies.

Some devices never transmit the data they collect: to retrieve the data, the adversary needs to physically access them.

See also

- Ears and Eyes[13].
- The hidden devices topic[14].

4.3.1. Audio

A microphone found inside a neon ceiling light in Modena, Italy, in December 2015[15].

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

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[60].

2013 case against Mónica and Francisco (#2): During a raid on the home of Mónica and Francisco, investigators found[45]:

- Several pieces of clothing and other accessories that Mónica and Francisco had used during the action and that were visible on public CCTV footage.
- Several unencrypted digital storage devices that contained suspicious documents.

Case against Jeff Luers (#2): During the raid of the storage unit, investigators found[55]:

- 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. 15)**, **Incrimination (p. 15)**

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. 36)**, 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 (#2): If possible, you can avoid answering questions or providing biometric information (face photograph, fingerprints, DNA) during ID checks.

Fake ID (#2): During an ID check, if providing your real identity could lead to your arrest or other negative consequences, you can present a fake ID (as long as the fake ID is not recognized as such by the State).

Repressive operations

Case against Boris (#2): 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[21].

4.12. Increased police presence

Used in tactics: **Arrest (p. 15)**, **Deterrence (p. 15)**

Increased police presence is the process by which 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. 39)** 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 around the demonstration or around its expected targets. This clustering can be an opportunity for them to conduct **overt surveillance (p. 39)** before, during, and after the demonstration.

Mitigations

Attack (#2): If you expect the police to increase their presence at a public demonstration, you can organize to make sure the crowd is large and fierce enough: decen-

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

If guards detect an unauthorized presence in the area under their watch, they 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 (#2): Before or during an action, you can incapacitate guards to prevent them from interfering with the action. For example, in their actions on logging companies machinery in so-called Chile, Mapuche people have neutralized guards by disarming them[56], tying them up[57] or shooting at them[58].

Reconnaissance (#2): Before an action, you can identify the presence of guards at the action site.

4.10. House raid

Used in tactics: **Arrest (p. 15)**, **Incrimination (p. 15)**

A house raid is a surprise search of a residence conducted by an adversary. An adversary often conducts a house raid early in the morning when the occupants of the residence are asleep and taken by surprise.

When

An adversary can conduct a house raid on a residence:

- Most often, early in the morning when the occupants of the residence are asleep and taken by surprise.
- In some cases, during the day. This can be the case when one goal of the raid is to seize digital devices while they are turned on (and therefore their **encryption (#2)** is not effective). In this case, the adversary can decide to conduct the house raid during the day because digital devices are more likely to be turned on when their users are awake, which is more likely to be during the day.

Why

An adversary can conduct a house raid on a residence to:

- Seize items to find evidence or to achieve **network mapping (p. 36)**. Commonly seized items include electronic devices, literature, materials that could be used in actions, and clothing. In some cases, the adversary seizes expensive items (e.g., computers, printing equipment) with the goal of disrupting the organizational capacity of their targets.
- Arrest the occupants of the residence.
- Install **covert surveillance devices (p. 17)** in the residence.

Additional considerations

In some countries, when they conduct a house raid, the State is only allowed to search the rooms of those named in a warrant.

Mitigations

Clandestinity (#2): If you enter clandestinity, an adversary cannot know where you live, and therefore cannot raid your home.

Preparing for house raids (#2): 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 (#2): You can prepare for repression to minimize the impact of house raids.

Stash spot or safe house (#2): You can keep action materials that have no "legitimate" purpose in a stash spot or safe house, or at worst, let them pass through your home only for a very limited time.

Repressive operations

Scripta Manent (#2): One comrade was arrested after batteries and an electrician's manual were found in his home during a raid[59].

Renata (#2): 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[27].

Repression of Lafarge factory sabotage (#2): Among the initial house raids, one was particularly thorough: cops

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

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

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

[59] 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

Covert audio surveillance devices are electronic devices, typically microphones, hidden by an adversary to collect audio data.

An adversary can hide covert audio surveillance devices anywhere interesting audio data, typically conversations, can be collected. Notable locations include:

- The living room of a target.
- The dashboard of the vehicle of a target.
- An outdoor location where a target regularly meets or is expected to meet other people.

Covert audio surveillance devices can be very sensitive and successfully pick up conversations even when there is loud music playing in the background or people are whispering. They 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. 36)**.

See Ears and Eyes[13] and the hidden devices topic[14].

Mitigations

Bug search (#2): You can conduct a bug search to locate covert audio surveillance devices and eventually remove them.

Outdoor and device-free conversations (#2): You can conduct sensitive conversations outdoors and without electronic devices to prevent an adversary from recording those conversations with covert audio surveillance devices.

Physical intrusion detection (#2): An adversary often needs to covertly enter a space to install a covert audio surveillance device in the space. You can use physical intrusion detection to detect such a covert entry.

Repressive operations

Renata (#2): Six hidden microphones and a camera were found in a house after the operation[16]. 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[17].

Scintilla (#2): Microphones hidden in a house for two and a half years recorded conversations that the investigators used to prove that the accused comrades knew each other, talked regularly, worried about the creation of a DNA database and the impossibility of resisting DNA collection, and discussed writing a text to be published[18].

See the corresponding Ears and Eyes case[19].

4.3.2. Location

A GPS tracker found under a vehicle in Berlin, Germany, in August 2022[20].

Covert location surveillance devices are electronic devices hidden by an adversary to collect location data.

An adversary typically hides covert location surveillance devices in or on a target's usual means of transportation, such as a car or bike.

Covert location surveillance devices need a way to determine their own location. They do this:

- Most often using GPS.
- In some cases, using alternatives to GPS such as GLONASS or satellite phone services.
- In rare cases, by emitting radio waves that are received by a nearby surveillance operator (typically in a vehicle following the target's vehicle).

Collected location data can be used as evidence in court. Non-incriminating, mundane location data can reveal a

[15] https://notrace.how/earsandeyes/#modena-2015-12

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

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

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

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

[20] https://notrace.how/earsandeyes/#berlin-2022-08

lot about the targets of surveillance and help in **network mapping (p. 36)**.

See Ears and Eyes[13] and the hidden devices topic[14].

Mitigations

Bug search (#2): You can conduct a bug search to locate covert location surveillance devices and eventually remove them.

Physical intrusion detection (#2): An adversary often needs to covertly enter the space where a vehicle is parked to install a covert location surveillance device on the vehicle. You can use physical intrusion detection to detect such a covert entry.

Transportation by bike (#2): You can use a bike instead of any other type of vehicle: unlike other vehicles, when you conduct a **bug search (#2)** of a bike you can determine with a high degree of confidence whether or not a covert location surveillance device is installed on the bike.

You should store the bike indoors to make it harder for an adversary to install a covert location surveillance device on it.

Repressive operations

Case against Boris (#2): 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[21].

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.

4.3.3. Video

A camera found in the skylight of a public school in Berlin, Germany, in July 2011[22].

Covert video surveillance devices are electronic devices, typically cameras, hidden by an adversary to collect video data.

An adversary can hide covert video surveillance devices anywhere with a line of sight to the target or area under surveillance. Notable locations include:

- The living room of a target.
- The windows of a building close to the home of a target, with a line of sight on the entrance of the home.
- Close to **stash spots or safe houses (#2)** as has happened in Italy, where motion-activated hunting cameras were installed to monitor a forest stash spot[23].

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. 36)**.

See Ears and Eyes[13] and the hidden devices topic[14].

Mitigations

Bug search (#2): You can conduct a bug search to locate covert video surveillance devices and eventually remove them.

Digital best practices (#2): An adversary can install covert video surveillance devices that can film a computer or phone screen, or a computer keyboard. To mitigate this, when using a computer or phone for sensitive activities, you can:

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

[22] https://notrace.how/earsandeyes/#berlin-2011-07

[23] 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

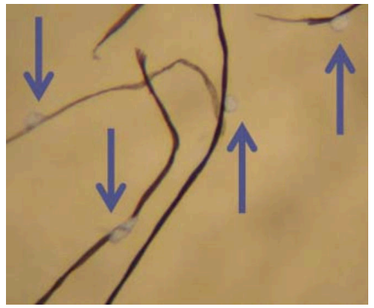
Biometric concealment (#2): You can hide the acoustic properties of your voice to conceal it.

Masking your writing style (#2): You can mask your writing style to mitigate author identification.

Repressive operations

Scripta Manent (#2): Texts published by some of the accused comrades were compared with action claims by the Informal Anarchist Federation, with the aim of proving that the comrades had written these claims[50].

4.8.10. Trace evidence



Spray paint droplets adhering to the fibers of a jacket, observed under a microscope (magnification ~75x). When spraying from a spray paint can, paint droplets from the resulting mist are likely to fall on nearby surfaces, and can be used to link clothing to paint found at an action site[53].

Trace evidence is the tiny fragments of physical evidence that can be transferred between objects, or between objects and the environment. This transfer can occur 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[54].

[53] *Handbook of Trace Evidence Analysis* (2020), chapter *Paints and Polymers*, p. 157–218.

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

Mitigations

Anonymous dress (#2): An adversary can use trace evidence from clothing (e.g., textile fibers detaching from clothing into the environment) to establish links between people, clothing, and places. To mitigate this, you can dress anonymously.

Careful action planning (#2): An adversary can use trace evidence to link objects to an action site. To mitigate this, you can carefully plan the action so that after the action you dispose of any tools or clothing you used during the action.

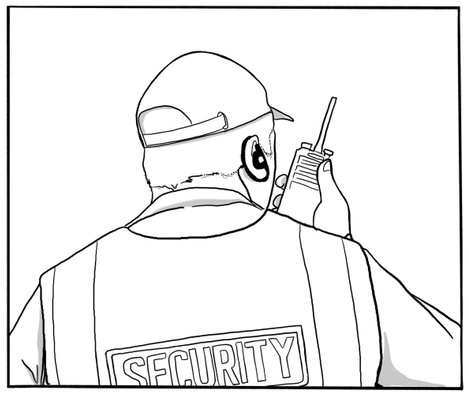
Stash spot or safe house (#2): An adversary can use trace evidence to link objects to an action site. To mitigate this, you can carefully plan the action so that after the action you store in a stash spot or safe house any tools that are too expensive to realistically discard after each action.

Repressive operations

Case against Jeff Luers (#2): 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[55].

4.9. Guards

Used in tactics: **Arrest (p. 15)**



Guards (also known as *security guards*) are people employed by an adversary to protect buildings or other physical infrastructure.

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

corresponding characteristics of a person recorded by the surveillance cameras of the police station[47].

Scintilla (#2): 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[4849].

4.8.8. Handwriting analysis

Handwriting analysis is the analysis of handwriting samples, typically for the purpose of matching one sample to another.

Handwriting analysis is based on an understanding 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.

Mitigations

Biometric concealment (#2): You can write on digital devices instead of by hand to conceal your handwriting. For example, when writing graffiti, you can use only uppercase letters and make the lettering as generic as possible.

Repressive operations

Scripta Manent (#2): 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[50].

2019-2020 case against Mónica and Francisco (#2): The labels on the two parcel bombs remained intact—one because the parcel didn't explode, and one despite the explosion of the parcel[33]. The handwritten signatures on the labels were compared and positively matched. This showed that the parcels were sent by the same person.

Repression of the first Jane's Revenge arson (#2): A comparison between the cursive graffiti left at the action site and the same style of graffiti painted a few months later during a demonstration helped identify the comrade who was later arrested[40].

4.8.9. Linguistics

Forensic linguistics is the application of linguistic knowledge 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

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

- Who wrote an anonymous action claim posted on the Internet or sent to a newspaper.
- Whether multiple anonymous action claims were likely written by the same person or group.
- Who wrote a plan describing illegal activities found during a **house raid (p. 29)**, a **covert house search (p. 16)** or an arrest.

Voice identification

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. 17)**.
- Who called the authorities to make a bomb threat.

See also

On the topic of author identification:

- Counteracting Forensic Linguistics[51].
- Who wrote that?[52].

Mitigations

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

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

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

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

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

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

- Keep the device facing a wall that you can thoroughly search for covert video surveillance devices (rather than facing a window or TV, for example).
- Enter your passwords while under an opaque sheet or blanket.

Physical intrusion detection (#2): An adversary often needs to covertly enter a space to install a covert video surveillance device in the space. You can use physical intrusion detection to detect such a covert entry.

Stash spot or safe house (#2): You can keep action materials in a stash spot or safe house to avoid bringing them into your home, where covert video surveillance devices can be present.

Surveillance detection (#2): An adversary can park a surveillance vehicle near your home with a camera that films your home entrance. To mitigate this, you can use the following passive surveillance detection technique. It 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 (#2): 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[21].

4.4. Detection dogs

Used in tactics: **Arrest (p. 15)**, **Incrimination (p. 15)**

Detection dogs are dogs that have been trained by an adversary to detect certain substances, primarily through their sense of smell.

An adversary can bring detection dogs to an action site shortly after the action and have them follow a scent. If the dogs successfully detect and follow 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 detection dogs to follow a scent in rural areas than in urban areas with higher population densities.

Mitigations

Careful action planning (#2): If you think that detection dogs can be deployed after an action, you can plan to take measures when leaving the action site. For example, you can plan to cross bodies of water to break the scent trail that the dogs are following, or plan to use pepper spray on the trail to disrupt the sense of smell of the dogs.

4.5. Door knocks

Used in tactics: **Deterrence (p. 15)**, **Incrimination (p. 15)**

Door knocks are when an adversary comes knocking where you live to intimidate you or get information. Door knocks aim to intimidate or create paranoia, to see who is willing to talk and possibly be recruited as an **informant (p. 31)**, 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. 36)**.

In many countries, it is easier for the State to carry out door knocks than **house raids (p. 29)** because door knocks do not require a warrant or legal authorization.

Mitigations

Avoiding self-incrimination (#2): If an adversary knocks on your door, you can avoid talking to them: instead, alert your networks and consider making the event public.

Digital best practices (#2): You can follow digital best practices to make it harder for an adversary to log who you contact after they knock on your door.

Repressive operations

Scintilla (#2): In May 2019, cops knocked on Boba's door under the pretext of giving a verbal notice to another comrade[24]. 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. 15)**

Evidence fabrication is the creation of fake evidence, or the falsification of existing evidence, to incriminate a target.

Notable examples of evidence fabrication include:

- Lying in a police report.
- Planting incriminating materials. 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.
- The common practice of investigators, prosecutors, and judges to "make up a story", by 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 you, because enough information (even mundane information) can be woven into a narrative for their purposes.

Depending on the context, evidence fabrication can be common or rare.

Mitigations

Need-to-know principle (#2): You can apply the need-to-know principle to limit the information an adversary has about your life, and therefore make it harder for the adversary to fabricate evidence.

Physical intrusion detection (#2): An adversary often needs to covertly enter a space to plant evidence in the space. You can use physical intrusion detection to detect such a covert entry.

4.7. Extra-legal violence

Used in tactics: **Deterrence (p. 15)**, **Incrimination (p. 15)**

Extra-legal violence is the use of physical and psychological force by the State outside of what is legally permitted.

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:[25].

In some contexts, extra-legal violence can include extra-legal assassinations.

Mitigations

Preparing for repression (#2): If you think you are at risk of being tortured if you are arrested, you can prepare for that risk. For example:

- You can prepare psychologically.
- You can set 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.

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

[25] 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.

2019-2020 case against Mónica and Francisco (#2): In order to identify Mónica and Francisco 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[33].

2013 case against Mónica and Francisco (#2): The main evidence against Mónica and Francisco was a comparison of photos of both of them with public CCTV footage that showed their uncovered faces while they were in the subway, shortly before or after the action[45].

4.8.6. Fingerprints

Ridges on a human finger.

Fingerprint forensics is the collection, storage and analysis of the impressions left by the ridges of human fingers.

Fingerprints are left on surfaces you touch by the moisture and grease on your fingers, and can be collected from these surfaces. They can also be collected directly from your 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[46].

Mitigations

Careful action planning (#2): An adversary can use fingerprint forensics to collect and analyze fingerprints at an action site. To mitigate this, you can carefully plan the action so that any tools you plan to use during the action are free of fingerprints in case you lose them or have to discard them in a location where they can be recovered by an adversary.

Gloves (#2): You can wear gloves to avoid leaving fingerprints on surfaces you touch.

4.8.7. Gait recognition

Gait recognition is the analysis of the walking style and pace of individuals, for the purpose of matching one walking style and pace to another.

Gait recognition involves a human or automated system locating and measuring the body features (e.g., position of the ankles, knees, and hips) of a person as they move, and comparing them with the body features of another person. If the body features are sufficiently similar, the bodies are considered to belong to the same person.

Modern gait recognition systems are capable of identifying a person from a great distance, even if they are deliberately trying to change their gait.

Mitigations

Anonymous dress (#2): You can wear baggy clothing to conceal your gait.

Biometric concealment (#2): You can wear baggy clothing that hides your body shape, use an umbrella or other concealing objects, or drastically change your walking style by adopting a "funny walk".

Repressive operations

Bialystok (#2): 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

[45] https://notrace.how/documentation/monica-and-francisco-2013-case-file.pdf

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

Panico (#2): DNA traces were the only evidence against one of the accused comrades[43].

4.8.4. Digital

A Cellebrite Universal Forensics Extraction Device (UFED) extracting data from an iPhone 4S, 2013.

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 (#2): An adversary can use digital forensics to retrieve self-incriminating information from a digital device. To mitigate this, you can avoid storing such information on digital devices except for very deliberate reasons (such as writing and sending an action claim while following **digital best practices (#2)**).

Digital best practices (#2): An adversary can use digital forensics to retrieve data from a computer you have used. To mitigate this, you can follow digital best practices and, in particular, use Tails[9], an "amnesic" operating system designed to leave no trace on the computer it runs on.

When investigating a cyber action, an adversary can use digital forensics to analyze the targets of the action to determine where the action came from, a process called *attribution* which may include determining what tools were used in the action and any other digital "signatures". When carrying out a cyber action, you can follow digital best practices to make it harder for an adversary to achieve attribution. For example, you can:

- Use popular rather than custom tools.
- If you use Virtual Private Servers (VPSs), **purchase them anonymously (#2)** and access them through Tails[9].

Encryption (#2): An adversary can use digital forensics to retrieve data from unencrypted digital devices. To mitigate this, you can encrypt your digital devices with Full Disk Encryption and a strong password.

Metadata erasure and resistance (#2): An adversary can use digital forensics to retrieve and analyze metadata. To mitigate this, you can erase metadata from files before publishing them online or sending them to others.

4.8.5. Facial recognition

Facial recognition is the analysis of the features of human faces for the purpose of matching one face to another.

Facial recognition involves a human or automated system locating and measuring the facial features (e.g., shape of the nose, distance between the eyes) of a face (or image of a face), and comparing them with the facial features of another face (or image of a face). If the features of the two faces are sufficiently similar, the faces are considered to belong to the same person.

Modern facial recognition systems are capable of matching a face image against a large database of faces, even if the face in the image is masked, with only the eyes and eyebrows visible. Facial recognition systems coupled with **mass video surveillance (p. 34)** can be used to automate the tracking of individuals through a space.

See the facial recognition topic[44].

Mitigations

Anonymous dress (#2): 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 (#2): 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

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

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

- 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 (#2): 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[26]. Most of the defendants who were tortured later retracted their statements and spoke publicly about the torture they had received.

Renata (#2): 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[27].

Belarusian anarcho-partisans (#2): The anarchists were tortured in the first days of their detention[28].

Repression of the 2019 uprising in Chile (#2): 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[29].

4.8. Forensics

Used in tactics: **Incrimination (p. 15)**

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.

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

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

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

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

4.8.1. Arson

Arson forensics (also known as *fire investigation*) is the application of science to the investigation of arson. Arson forensics has 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 involves determining whether a fire was intentionally set and identifying its point of origin. It becomes much more difficult when the "flashover" point has been reached—when a room becomes so hot that every ignitable surface bursts into flames.

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 (p. 20)** at the scene.

Mitigations

Anonymous purchases (#2): An adversary can sometimes identify accelerants and trace them back to a gas station brand, and from there to the identity of the person who purchased the accelerants. To mitigate this, you can purchase accelerants anonymously.

Careful action planning (#2): An adversary can tie actions together if accelerants from the same sources are used in all of them. To mitigate this, you can avoid reusing accelerants from the same source in different actions.

4.8.2. Ballistics

On the left, an unfired 9mm bullet. On the right, a fired bullet of the same model.

Ballistic forensics (also known as *firearm examination*) is the application of science to the investigation of firearms and bullets. 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.

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

Mitigations

Anonymous purchases (#2): An adversary can use ballistic forensics to trace back a firearm or bullet to a seller, and from there to the identity of the person who purchased the firearm or bullet. To mitigate this, you can purchase firearms and bullets anonymously, for example through connections to organized criminal networks or through fraud.

Stash spot or safe house (#2): An adversary needs to have access to a firearm to perform a ballistic analysis on the firearm. To prevent this, you can store the firearm in a stash spot or safe house.

4.8.3. DNA

DNA forensics (also known as *DNA analysis*) is the collection, storage, and analysis of DNA traces for the purpose of matching DNA traces to individuals.

Collection

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

Analysis

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.

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.

DNA databases

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.

See also

- Dna You Say? Burn Everything to Burn Longer: A Guide to Leaving No Traces[30] for a comprehensive overview of DNA forensics literature.
- The DNA topic[31].

Mitigations

Careful action planning (#2): An adversary can use DNA forensics to collect DNA at an action site. To mitigate this, you can carefully plan the action to minimize DNA traces at the action site. For example, you can:

- Secure your hair under a hat.
- If you have to cut a fence, cut any fence holes large enough to pass through without touching the fence.
- Ensure that surfaces at the action 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 (#2)**.
- Ensure 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.
- Ensure that nothing is accidentally left behind such as a bag, tool, or anything that falls out of a pocket.

DNA minimization protocols (#2): You can minimize the amount of DNA you leave on a surface to minimize the risk that an adversary can use DNA forensics to draw a valuable conclusion from an analysis of the surface.

Gloves (#2): You can wear gloves to avoid leaving DNA on surfaces you touch.

Repressive operations

Scripta Manent (#2): DNA evidence was used to convict Alfredo Cospito[32].

Case against Boris (#2): 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[21].

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.

2019-2020 case against Mónica and Francisco (#2): Francisco's DNA was allegedly found on the parcel bomb sent to the former Minister of the Interior, which was defused and didn't explode[33].

Repression against Zündlumpen (#2): 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[34].

Renata (#2): 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[35]. 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 (#2): 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[36]. One person who refused to wear a mask had their underwear confiscated while in police custody, presumably for DNA collection[37].

Prometeo (#2): DNA traces were used to convict the comrade accused of burning an ATM[38].

Mauvaises intentions (#2): During police custody, DNA was collected from the comrades' clothing and from plastic cups[39]. 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 (#2): In May 2022, DNA traces were collected from several items found by investigators at the action site, including a broken window, a glass jar, a lighter, and an intact Molotov cocktail[40]. 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 action site.

Scintilla (#2): 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[41].

Nea Filadelphia case (#2): 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[42].

[30] https://notrace.how/resources/#dna-you-say
[31] https://notrace.how/resources/#topic=dna
[32] 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
[33] https://notrace.how/resources/#uber-orwell-und-der-fall-von-monica-und-francisco
[34] https://notrace.how/resources/#die-verfolgung-von-anarchist-innen-und-kippenstummeln-im-bajuwarisch-christlichen-konigreich
[35] https://roundrobin.info/2020/03/aggiornamenti-su-manu-stecco-juan-e-sasha
[36] https://sansnom.noblogs.org/archives/16831
[37] https://notrace.how/resources/#affaire-lafarge-les-moyens-denquetes-utilises
[38] https://roundrobin.info/2021/05/sentenza-beppe
[39] https://infokiosques.net/spip.php?article597
[40] https://notrace.how/documentation/first-jane-s-revenge-arson-investigation-files.pdf
[41] https://roundrobin.info/2019/12/verona-una-perquisizione-e-un-arresto
[42] https://abcsolidaritycell.espivblogs.net/archives/130