Threat Library

The Threat Library is a knowledge base of repressive techniques, mitigations that can be taken to counter them, and repressive operations where they've been used. The goal is to help anarchists and other rebels understand the options available to their adversaries, develop appropriate threat models, and ultimately succeed in their actions and projects.

Part 2/2

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.

November 4, 2025

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

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.

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

Original text in English

No Trace Project

notrace.how/threat-library

8. Contribute to the Threat Library

8.1. Contact

Is there a **technique (#1)**, **mitigation (p. 5)**, or **repressive operation (p. 25)** that you think is missing? Would you like to edit one that is currently listed? To contribute to the Threat Library with additions, improvements, criticism, or feedback, get in touch with us:

notrace@autistici.org (PGP[170])

8.2. Repressive operations

The Threat Library aims to reference repressive operations that have targeted anarchists or other rebels anywhere in the world, and that feature interesting repressive techniques that are representative of local State repression. In order to diversify our coverage we are particularly looking for operations outside of Western Europe and North America, but we welcome contributions from these regions as well.

8.3. Translations

To translate the Threat Library to a new language or improve an existing translation, see this page.[171]

[170] https://notrace.how/notrace.asc
[171] https://notrace.how/translations.html

Contents

- 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 (p. 49)** for more information.

7.3. 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 (#1)** 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).

7.3.1. 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.

7.3.2. Likelihood

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

7.3.3. 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.

7.3.4. 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 (p. 15)** when committing arson, you become less vulnerable to DNA forensics.

7.3.5. 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 (p. 25)** can help you gain an understanding of how a given technique is used in a given context.

7.4. Additional tips on using the Threat Library

The Threat Library Matrix[169] provides an overview of all the 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 them. If you follow our suggested process above and draw your own attack tree, the overview can help you think of relevant techniques that are missing from your tree.

The Threat Library welcomes external contributions, such as:

[169] https://notrace.how/threat-library/matrix.html

4. Mitigations

4.1. Anonymous dress

Techniques addressed by this mitigation:

Forensics > Facial recognition (#1)
Forensics > Gait recognition (#1)
Forensics > Trace evidence (#1)
Mass surveillance > Civilian snitches (#1)
Mass surveillance > Video surveillance (#1)
Physical surveillance > Aerial (#1)
Physical surveillance > Overt (#1)

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

Hide your body features

To hide your body features, you can:

- To hide your face: wear a mask that adequately covers your face, including your eyebrows and up to the top of your nose.
- To hide the rest of your body: wear a shirt with long sleeves, gloves, pants with long legs, and high socks.
- To hide your skin color: make sure no skin is visible, including around your eyes, at the junction of your shirt and gloves, and at the junction of your pants and socks.
- To hide your body shape and gait: wear baggy clothing (you can also conceal your gait with **biometric concealment (p. 9)**).

Ensure that clothing cannot be used to identify you

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

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

The "black bloc"

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

4.2. Anonymous phones

Techniques addressed by this mitigation:

Network mapping (#1)
Service provider collaboration > Mobile network operators (#1)

An anonymous phone is a phone that is not tied to your identity. A burner phone is an anonymous phone that you discard shortly after use.

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.

7.2.4. 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.

7.2.5. Burn or digitize your notes

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

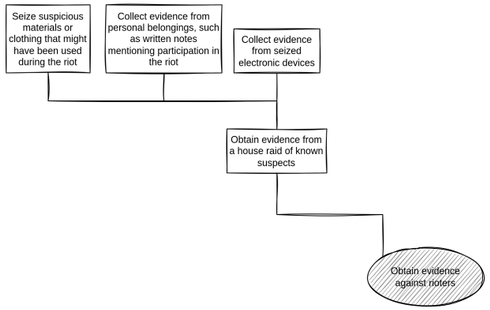
1. At the end of the exercise, memorize your notes and then burn them. This approach makes it difficult to later revisit your notes and expand them.
2. At the end of the exercise, digitize your notes by manually copying them to an encrypted USB device using Tails[15] (remember to follow **digital best practices (p. 12)**). 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.

7.2.6. 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 (p. 19)**, you discuss what went well and what went wrong, and whether there is room for improvement in the coverage of your attack tree or how you implemented the mitigations.

7.2.2. 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 (#1)**.
- "Collect evidence from seized electronic devices" matches **Targeted digital surveillance: Physical access (#1)** because they would access your electronic devices, and **Targeted digital surveillance: Authentication bypass (#1)**, 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. 47 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.

7.2.3. Identify mitigations

Next, you identify 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 (p. 20)**, **Preparing for house raids (p. 20)** and **Stash spot or safe house (p. 21)**. You don't want to implement **Clandestinity (p. 11)** because you decide against going down that road.
- For the two "Targeted digital surveillance" techniques, **Digital best practices (p. 12)** is the only mitigation that makes sense in your context.

You update the table (7).

Anonymous phones

You can use anonymous phones for sensitive projects or actions where you have determined that the need for a phone is unavoidable. Unless the phone numbers need to be stable in the long term, you should always prefer burner phones.

To setup and use an anonymous phone:

- **Anonymously purchase (p. 6)** the phone, its SIM card, and its plan.
- Do not turn on the phone close to where you live, because an adversary can learn the history of a phone physical location with the **collaboration of mobile network operators (#1)**.

Pseudo-anonymous phones

Pseudo-anonymous phones are phones that you have purchased anonymously but you use close to where you live. They can mitigate **network mapping (#1)**—especially if all members of a scene or network use them—but you should not use them for sensitive projects or actions.

See also

- AnarSec's guide "Kill the Cop in Your Pocket"[1] on the dangers of using a phone.
- Burner Phone Best Practices[2] for more information on burner phones.

4.3. Anonymous purchases

Techniques addressed by this mitigation:

Forensics > Arson (#1)
Forensics > Ballistics (#1)
Forensics > Trace evidence (#1)
Mass surveillance > Video surveillance (#1)
Service provider collaboration > Other (#1)

Anonymous purchases is the practice of purchasing items without associating your identity with the purchase.

You should anonymously purchase any items you plan to use for an action. This way:

- If an adversary finds the items at the action site (e.g., an incendiary device with a delay that failed) or traces of the items (e.g., traces of accelerant discovered by **arson forensics (#1)**) and discovers where the items were purchased, they will not discover your identity.
- If an adversary obtains your bank records through the **collaboration of your bank (#1)**, they will not discover the purchase.

Physical anonymous purchases

To anonymously purchase an item in a physical store:

- Make the purchase some time before you need to use the item (e.g. weeks or months before). This way, if an adversary finds the item and discovers where it was purchased, they will not be able to see you on recent CCTV footage of the store or the surrounding area.
- Make the purchase at a store that is not close to where you live.
- Go to the store using an anonymous mode of transportation (such as a **bike (p. 24)**), and do not bring a phone.
- Conduct **anti-surveillance (p. 7)** before going to the store.
- Use some level of **anonymous dress (p. 5)** to be less recognizable—a "Covid" mask, a hat, dedicated clothing.
- Pay in cash.
- Make sure your interaction with the cashier is not memorable.
- If you have to purchase several items, you can make the purchases in different stores, in different locations, at different times. This is especially important if you purchase items that would be suspicious to purchase together.

Digital anonymous purchases

You can make digital anonymous purchases with cryptocurrencies. You should either acquire the cryptocurrencies anonymously, or sufficiently launder them before using them, which can be a hassle, but is possible with cryptocurrencies like Monero using Tails.

[1] https://anarsec.guide/posts/nophones
[2] https://notrace.how/resources/#burner-phones

See also

See PRISMA[3] for more details on physical anonymous purchases.

4.4. Anti-surveillance

Techniques addressed by this mitigation:

Physical surveillance > Aerial (#1)
Physical surveillance > Covert (#1)

Anti-surveillance is the practice of taking active measures to evade ("shake off") a **mobile physical surveillance operation (#1)**.

When to conduct anti-surveillance

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

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

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

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

A core principle

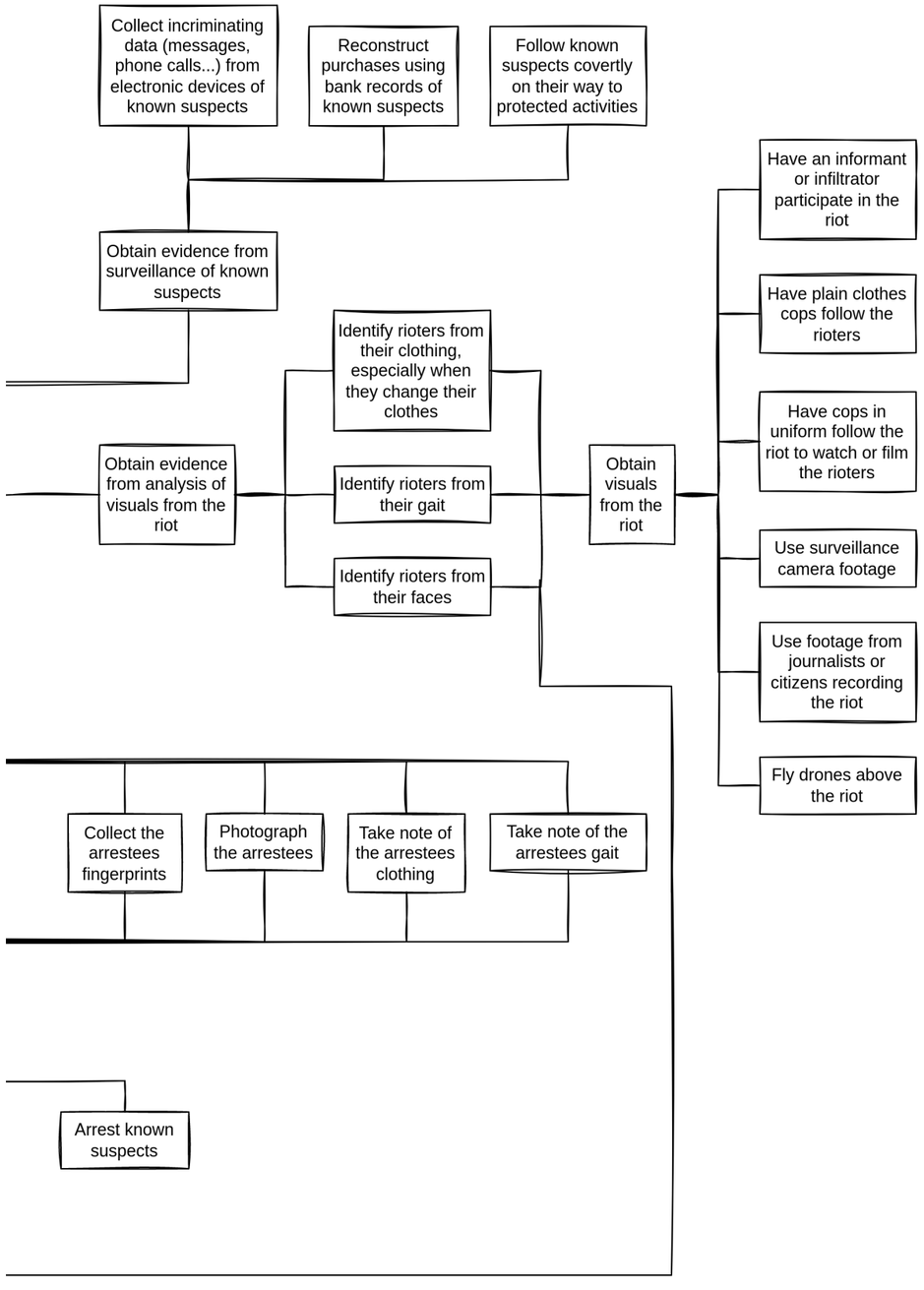
A core principle of anti-surveillance is that, usually, a surveillance operation really doesn't want to be detected by its target, and would rather lose its target than risk detection. Because of this, most anti-surveillance measures you take should attempt to provoke one of two situations: either the surveillance operators expose themselves in a way that you can detect, or they lose you. You should remain observant while taking an anti-surveillance measure, so that you can detect operators who have exposed themselves because of the measure.

Examples

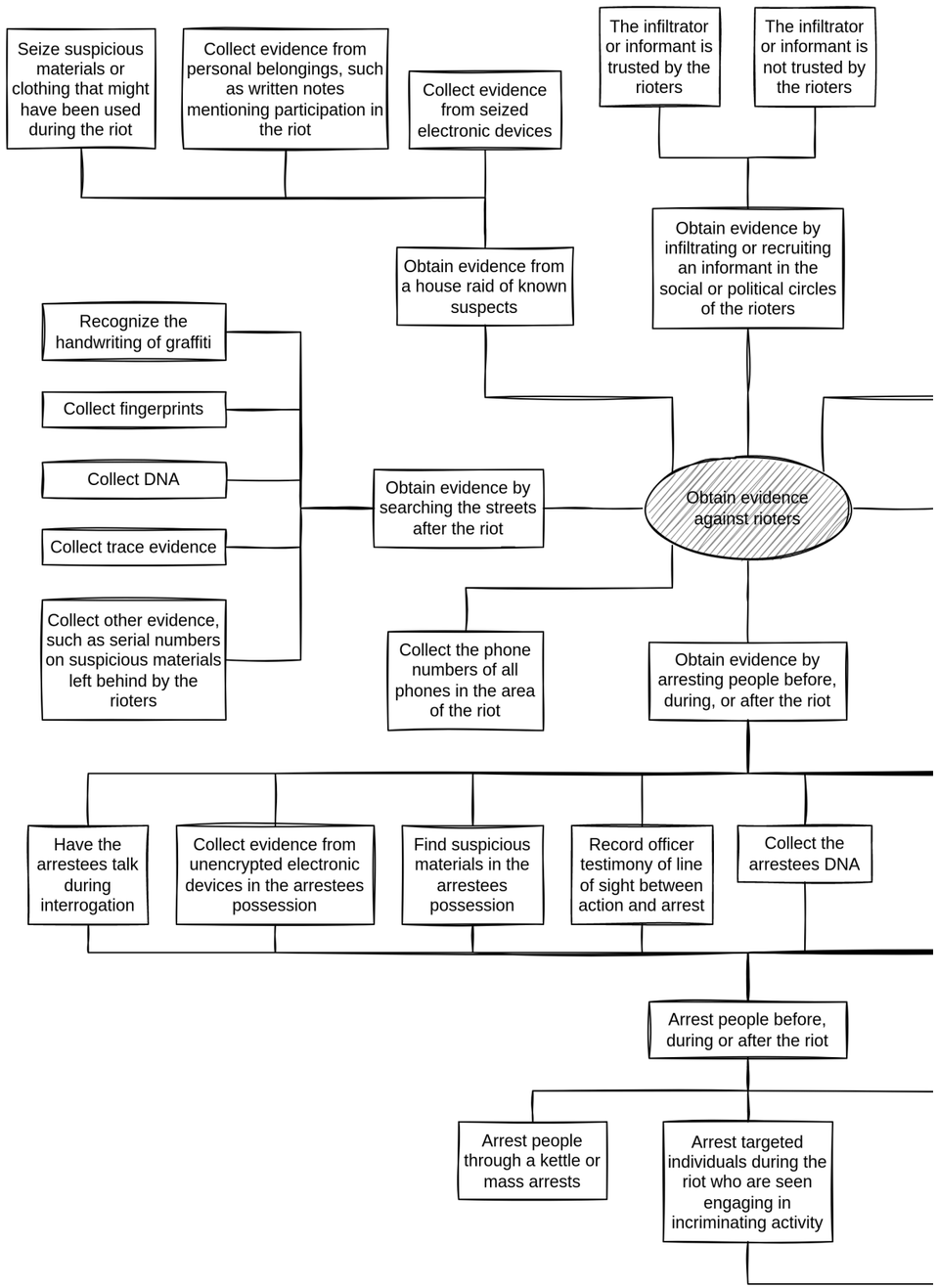
Anti-surveillance is an advanced practice. Before conducting anti-surveillance, we recommend that you read up on it using the links at the end of this description. That said, examples of anti-surveillance include:

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

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



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



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

of the forest far from where you entered, in a place that a surveillance operation would not expect. If you notice people acting strangely as you enter or exit the forest, they may be surveillance operators.

Additional considerations

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

See also

- Surveillance Countermeasures[4] about the principles and techniques of anti-surveillance.
- The "Physical surveillance" topic.[5]
- The related mitigation **Surveillance detection (p. 22)**.

4.5. Attack

Techniques addressed by this mitigation:

Alarm systems (#1)
Guards (#1)
Increased police presence (#1)
Infiltrators (#1)
Informants (#1)
Mass surveillance > Civilian snitches (#1)
Mass surveillance > Police files (#1)
Mass surveillance > Video surveillance (#1)
Physical surveillance > Aerial (#1)
Police patrols (#1)
Roadblocks (#1)

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

Mass digital surveillance is impossible if the Internet backbone has been taken offline by cutting fiber optic cables. Video surveillance depends not only on network connectivity, but also on physical cameras that are too decentralized to effectively protect against sabotage. A witness can be intimidated into not testifying in an upcoming trial if the car outside their house is torched while they sleep. Informants and infiltrators can be immiserated and attacked in countless creative ways. Increased police presence somewhere means the possibility of decreased police presence somewhere else. Forensic labs can go up in smoke. Police communications depend on TETRA[6] and P25[7] antennas, and police operations depend on the integrity of their vehicle fleets, stations, and individual officers' feelings of safety. The possibilities for attack are limited only by one's imagination.

[4] https://notrace.how/resources/#surveillance-countermeasures
[5] https://notrace.how/resources/#topic=physical-surveillance

4.6. Avoiding self-incrimination

Techniques addressed by this mitigation:

Door knocks (#1)
Forensics > Digital (#1)
ID checks (#1)
Interrogation techniques (#1)
Mass surveillance > Mass digital surveillance (#1)
Network mapping (#1)
Open-source intelligence (#1)

Avoiding self-incrimination means not giving information to an adversary that could be used to incriminate you or your comrades. An enormous number of convictions are based on information obtained through self-incrimination.

Do not talk to the police

If you are arrested by the State, do not talk to the police. Any communication could be used to incriminate you or your comrades.

Exceptions to this rule include:

- In many contexts, you may be forced to provide the police with some form of identification (often your name, date and place of birth) to avoid arrest or other negative consequences.
- In some contexts, you may be forced to provide the police with your biometric information (face photograph, fingerprints, DNA).

See How to defend yourself during a police interrogation[8] on how to resist police interrogation techniques.

[6] https://en.wikipedia.org/wiki/TETRA
[7] https://en.wikipedia.org/wiki/Project_25
[8] https://notrace.how/resources/#police-interrogation

Need-to-know principle

Apply the **need-to-know principle (p. 18)**. In particular, do not brag about crimes to friends, comrades, or cellmates—even if you have a solid foundation of trust, the knowledge unnecessarily endangers the person you're telling and could be overheard by an adversary.

Digital best practices

Follow **digital best practices (p. 12)**. In particular:

- Do not let anything incriminating go through your phone (text messages, photos, etc.), even if you are using end-to-end encrypted messaging applications.
- Do not use social media, or at least do not post anything incriminating on social media. Social media is a treasure trove for the State.
- Do not take photos or videos during riots. Taking photos or videos during riots incriminates people and should be considered a form of snitching.[9]

4.7. Background checks

Techniques addressed by this mitigation:
Infiltrators (#1)
Informants (#1)

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

Performing a background check on someone may involve:

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

We recommend two different approaches to background checks:

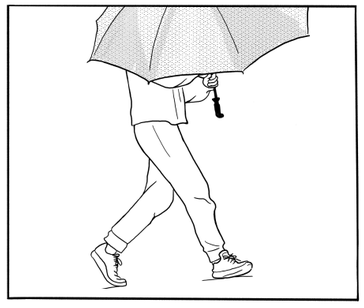
- The consensual, mutual approach: If you already trust someone to some degree but would like to trust them more, you can do a mutual background check, where each of you checks the other.
- The non-consensual approach: If you already have strong suspicions that someone is lying about their identity,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

See also:

- Confidence, Courage, Connection, Trust[10] on the use of ID checks to verify that someone is who they say they are.
- Handbook for Exposing an Undercover Cop[11] on a method for identifying, investigating and exposing undercover cops, including through using background checks.

4.8. Biometric concealment

Techniques addressed by this mitigation:
Forensics > Facial recognition (#1)
Forensics > Gait recognition (#1)
Forensics > Handwriting analysis (#1)
Forensics > Linguistics (#1)
Mass surveillance > Video surveillance (#1)



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

See the "Facial recognition" topic[12] and the chapter "Traces" in PRISMA.[3]

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

[10] https://notrace.how/resources/#confidence
[11] https://notrace.how/resources/#handbook-undercover-cop
[12] https://notrace.how/resources/#topic=facial-recognition

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

Let's say you and some comrades are preparing for a riot in a big city in the United States. You want to do some damage, but you don't want to get caught… You turn to the Threat Library for help. You print out this zine, take a pen and paper, and meet with your comrades **outdoors and without electronic devices (p. 19)**.

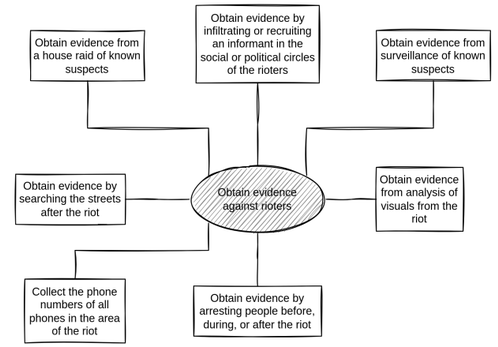
The goal of the discussion: draw an attack tree, identify techniques and mitigations that apply to your context, and decide how to implement those mitigations. After the riot, it may be a good idea to conduct an *action review*.

7.2.1. 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 riot to convince a judge to convict you. You draw an attack tree to represent the ways they could achieve this goal.[168] 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).

[168] 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).

7. 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*.[167]

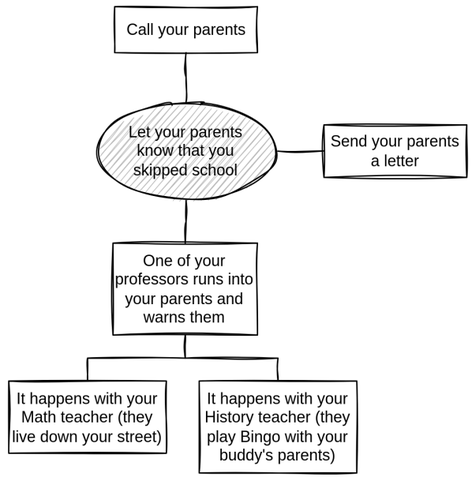
Attack trees are a tool to facilitate a brainstorming exercise on the different ways an adversary could successfully attack you in a given context by representing the attacks —the threats—in a tree structure. They help understand how a plan or project is vulnerable to repression by modeling the options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

7.1. 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.

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

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

4.9. Bug search

Techniques addressed by this mitigation:

Covert surveillance devices > Audio (#1)
Covert surveillance devices > Location (#1)
Covert surveillance devices > Video (#1)
Targeted digital surveillance > Authentication bypass (#1)
Targeted digital surveillance > IMSI-catcher (#1)

A bug search is the active process of trying to detect the presence of **covert surveillance devices (#1)** in a building, vehicle, or outdoor area. The primary technique in this process is a manual, visual search of the area. A secondary technique is to use specialized detection equipment.

Purpose of the search

Searching for bugs in a comprehensive and effective manner requires an extreme degree of technical expertise. If you do not have that expertise, when searching for bugs in an area, you cannot be sure that you have found all the bugs present in the area. Therefore, the purpose of searching for bugs should be to prevent an adversary from gathering information about you, not to consider an area free of covert surveillance devices. Incriminating conversations should always take place **outdoors and without electronic devices (p. 19)**.

Manual, visual search

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

- If you're searching a building, you can use appropriate tools to disassemble electrical outlets, multiple-socket adapters, ceiling lights, and any electrical appliances, looking for anything that shouldn't be there. You can also look inside furniture, basically anywhere a bug might fit.
- If you're searching a vehicle, you can look under the vehicle, inside the wheels, on the rear bumper, behind the vents, looking for anything that shouldn't be there. You can use appropriate tools to dismantle the interior, the ceiling, the dashboard, the seat heads, and so on. On motorcycles or bikes, you can look inside or under the seats. Unlike other vehicles, when searching a **bike (p. 24)**, you can determine with a high degree of confidence whether or not a bug is present.
- If you're searching for cameras installed at the windows of buildings on a street, you may be able to see such cameras with binoculars.
- If you're searching for cameras installed in surveillance vehicles on a street, you can detect such vehicles with **passive surveillance detection (p. 22)**.

Specialized detection equipment

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

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

See also

See Ears and Eyes,[13] a database of cases of covert surveillance devices used against anarchists and other rebels.

4.10. Careful action planning

Techniques addressed by this mitigation:

Detection dogs (#1)
Forensics > Arson (#1)
Forensics > DNA (#1)
Forensics > Fingerprints (#1)
Forensics > Gait recognition (#1)
Forensics > Trace evidence (#1)
Increased police presence (#1)
Mass surveillance > Civilian snitches (#1)
Police patrols (#1)
Roadblocks (#1)

When planning an action, careful action planning is the sensible development of the action plan. It follows **reconnaissance (p. 21)**.

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

Careful action planning must make clear the role of each person involved in the action and how their tasks relate to those of others.

For example, what is the best route to and from the action site, and how long will you be at the site, given the expected timing of the adversary's response? Or, what on your escape route could interfere with a pursuit (e.g., will the adversary need to get out of their vehicle to follow on foot)? Creating an action plan is a form of threat modeling—what could go wrong, what mitigations will you implement, and how? For example, how will you conduct **anti-surveillance (p. 7)** prior to the action meeting point?

4.11. Clandestinity

Techniques addressed by this mitigation:

Covert house visit (#1)
House raid (#1)

Clandestinity is the process of breaking away from your established identity and begin a new life with a **fake identity (p. 16)**.

You can enter clandestinity:

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

See the "Clandestinity" topic.[14]

4.12. Compartmentalization

Techniques addressed by this mitigation:

Network mapping (#1)
Targeted digital surveillance > Malware (#1)
Targeted digital surveillance > Network forensics (#1)

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

Examples of digital compartmentalization include:

- Using different email accounts for different digital identities, such as one account for work, another for friends, another for a specific sensitive project, etc. This way, if an adversary knows your work email address and discovers your sensitive email address after seizing a computer in a house raid, because the email addresses are different, they won't be able to link the sensitive email address to your identity.
- Using different Tails[15] USB sticks or Qubes OS[16] virtual machines for different digital identities. This way, if an adversary compromises one stick or virtual machine with **malware (#1)**, the compromise won't spread to other sticks or virtual machines.

Examples of non-digital compartmentalization include:

- Using different names in different contexts, such as using your civil name with your family and an alias with your friends. An alias can be specific to a place, time, or group of people you interact with. This way, if an adversary compromises one of your names, it won't necessarily lead to the compromise of the others.
- Applying the **need-to-know principle (p. 18)** by sharing sensitive information only when it is necessary to do so, and only to the extent necessary.

Compartmentalization can be a useful tool for remembering to apply mitigations consistently within a project. For example, you may want to always take **anti-surveillance (p. 7)** measures when traveling as part of a specific project, but not make the same effort for another, less sensitive project.

4.13. Computer and mobile forensics

Techniques addressed by this mitigation:

Targeted digital surveillance > Malware (#1)
Targeted digital surveillance > Physical access (#1)

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

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

[15] https://tails.net

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

6.13. Russia

Repressive operations:

Network (p. 32)
Case against Ruslan Siddiqi (p. 26)

6.14. Spain

Repressive operation:

2013 case against Mónica and Francisco (p. 34)

6.15. Sweden

Repressive operation:

Case against Revolutionära fronten (p. 34)

6.16. United States

Repressive operations:

Case against Marius Mason (p. 38)
Case against Jeff Luers (p. 37)
2011-2013 case against Jeremy Hammond (p. 35)
Search for a fugitive (p. 28)
Repression of the first Jane's Revenge arson (p. 26)
Case against Peppy and Krystal (p. 25)

6. Countries

6.1. Argentina

Repressive operation:
- **Repression of the attack on Clarín's headquarters (p. 27)**

6.2. Belarus

Repressive operation:
- **Belarusian anarcho-partisans (p. 27)**

6.3. Canada

Repressive operation:
- **Case against Direct Action (p. 38)**

6.4. Chile

Repressive operations:
- **2019-2020 case against Mónica and Francisco (p. 28)**
- **Repression of the 2019 uprising in Chile (p. 29)**

6.5. Czech Republic

Repressive operation:
- **Fenix (p. 34)**

6.6. Eswatini

Repressive operation:
- **Case against Amos Mbedzi (p. 36)**

6.7. France

Repressive operations:
- **Mauvaises intentions (p. 36)**
- **Bure criminal association case (p. 31)**
- **December 8 case (p. 30)**
- **Case against Boris (p. 27)**
- **Repression of Lafarge factory sabotage (p. 26)**
- **Case against Louna (p. 25)**

6.8. Germany

Repressive operations:
- **Repression against Zündlumpen (p. 28)**
- **The three from the park bench (p. 29)**
- **Berlin 2023 railway conspiracy case (p. 25)**

6.9. Greece

Repressive operation:
- **Nea Filadelphia case (p. 35)**

6.10. Italy

Repressive operations:
- **Scripta Manent (p. 37)**
- **Scintilla (p. 33)**
- **Panico (p. 32)**
- **Prometeo (p. 32)**
- **Renata (p. 32)**
- **Arrest of Stecco (p. 30)**
- **Bialystok (p. 31)**

6.11. New Zealand

Repressive operation:
- **Operation 8 (p. 36)**

6.12. Poland

Repressive operation:
- **Warsaw 3 (p. 33)**

If you suspect that one of your devices has been compromised and you want to learn more about the suspected compromise, you could ask for help from the non-profit organizations AccessNow[17] or Amnesty International,[18] with the caveat that they are legal organizations that might be forced to share with the State data that you provide them.

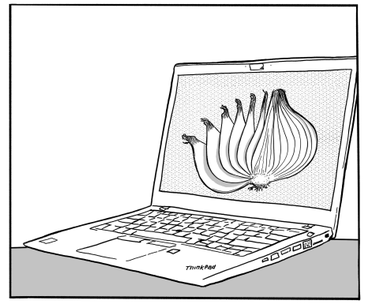
See also:

- The Device Integrity[19] page on Privacy Guides.
- Practical Linux Forensics[20] for a comprehensive introduction to the skill set on Linux, the platform most relevant to anarchists and other rebels.

4.14. Digital best practices

Techniques addressed by this mitigation:
- **Alarm systems (#1)**
- **Biased interpretation of evidence (#1)**
- **Covert surveillance devices > Video (#1)**
- **Door knocks (#1)**
- **Doxing (#1)**
- **Forensics > Digital (#1)**
- **Mass surveillance > Mass digital surveillance (#1)**
- **Network mapping (#1)**
- **Service provider collaboration > Mobile network operators (#1)**
- **Service provider collaboration > Other (#1)**
- **Targeted digital surveillance > Authentication bypass (#1)**
- **Targeted digital surveillance > Malware (#1)**
- **Targeted digital surveillance > Network forensics (#1)**
- **Targeted digital surveillance > Physical access (#1)**

[17] https://accessnow.org/help
[18] https://securitylab.amnesty.org/get-help
[19] https://privacyguides.org/en/device-integrity
[20] https://notrace.how/resources/#linux-forensics



The foundation of digital best practices is to limit the reach of technology into your life. Try to limit your use of digital devices, in particular for sensitive activities. That said, when using digital devices, you can follow the following best practices.

Do not use a phone, or leave your phone at home

A phone location is tracked at all times, its hardware identifiers and subscription information are logged by cell towers with every connection, and it can be hacked. If possible, do not use a phone. If you must use a phone:

- Use a GrapheneOS[21] smartphone with end-to-end encrypted messaging applications. Do not use traditional SMS and calls.
- Do not carry the phone with you, leave it at home at all times.

See AnarSec's guide "Kill the Cop in Your Pocket"[1] on the dangers of using a phone.

Use security-oriented operating systems

Use:

- Debian[22] or Qubes OS[16] for daily computer use. See AnarSec's guide "Qubes OS for Anarchists"[23] on Qubes OS.
- Tails[15] for sensitive computer use, such as reading a sensitive article, researching for an action, writing and sending an action claim, and moderating a sketchy website. See AnarSec's guides "Tails for Anarchists"[24] and "Tails Best Practices".[25]

[21] https://grapheneos.org
[22] https://debian.org
[23] https://anarsec.guide/posts/qubes
[24] https://anarsec.guide/posts/tails
[25] https://anarsec.guide/posts/tails-best

- GrapheneOS[21] for phones. See AnarSec's guide "GrapheneOS for Anarchists".[26]

Do not use:

- Windows, macOS, or iOS, as they are not open-source.
- Stock Android, as it is not as secure as GrapheneOS.

Encrypt your devices

Enable **Full Disk Encryption (p. 15)** on all your digital devices, and turn them off when you're not using them.

Use strong passwords

Most of your passwords (e.g. passwords you use to log in to websites) should be generated by and stored in a password manager—we recommend KeePassXC[27]—so that you don't have to remember them or even type them. They can be very long and random, say 40 random characters. You can generate such passwords with KeePassXC (select the "Password" tab when generating a password).

The passwords you enter when booting your encrypted devices and KeePassXC's password must be memorized. We recommend using Diceware[28] passwords of 5 to 10 words.[29] You can generate such passwords with KeePassXC (select the "Passphrase" tab when generating a password) or with physical dice.[30] You should use different passwords for each of your encrypted devices, but we recommend using the same password for all your KeePassXC databases (so that you have less passwords to memorize).

[26]https://anarsec.guide/posts/grapheneos

[27]https://keepassxc.org

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

[29]If an adversary physically accesses one of your digital devices, they can try to guess its password through repeated, automated authentication attempts (a process called "brute force"). They can also copy the device's data and wait years or decades until new technologies are invented that allow them to guess a password they cannot guess today. To mitigate this, you should use strong passwords. Assuming you are using the operating systems we recommend, and based on our best knowledge of the capabilities of State adversaries, we recommend that you use Diceware passwords of:

- 5 words to be safer *today*.
- 7 words to be safer *in the near future*.
- 10 words to be safer *in the distant future*.

[30]https://eff.org/dice

For example, if you have an encrypted laptop, a Tails stick and an encrypted phone, you will have to remember 4 passwords of 5 to 10 words (one for each device and one for the KeePassXC databases). This is a lot! To make sure you don't forget all those passwords, you can:

- Use memorization techniques, such as repeating the passwords in your head every day when you wake up.
- Store a copy of the passwords on a USB stick that you keep in a hidden place outside your home, and that is encrypted with a 10-word Diceware password. You don't memorize this 10-word password, you store it in the KeePassXC databases of one or two trusted comrades who also follow these digital best practices. This way, if you forget a password, you can ask the trusted comrades for the 10-word password and retrieve the USB stick: on it, you will find the forgotten password.
- Store a copy of the passwords on a USB stick that you keep in a hidden place outside your home, and that is encrypted with a 20-word Diceware password. You don't memorize this 20-word password, you split it into two halves of 10 words each, write each half on a piece of paper, and store each piece of paper in a different hidden place (not with the USB stick). This way, if you forget a password, you can retrieve the two pieces of paper, reconstruct the 20-word password, and retrieve the USB stick: on it, you will find the forgotten password.

Use Tor or a VPN

Use Tor[31] or a reputable Virtual Private Network (VPN) for your Internet activity. If you use Tor or a VPN and an adversary is monitoring your network traffic, it is harder for them to obtain data about your Internet activity, such as what websites you visit or what you do on those websites (it is also harder for them to target you with **malware (#1)**).

However, note that Tor and VPNs are not equivalent:

- If you use Tor, it is *very difficult*, even for the State, to obtain data about your Internet activity (as long as you otherwise follow digital best practices).
- If you use a VPN, it can be either difficult or easy for the State to obtain data about your Internet activity,

[31]https://torproject.org

Forensics > Trace evidence (#1)
House raid (#1)
Physical surveillance > Covert (#1)

On a night in June 2000, Jeff Luers and Craig Marshall were arrested in Oregon, United States, accused of setting fire to three trucks at a Chevrolet dealership earlier that night.[160] Jeff Luers was later also charged with an attempted arson of trucks at a petroleum products distributor in May 2000.

The June arson charge was based in part on a physical surveillance operation conducted on the night of the arson. The May arson attempt charge was based in part on incendiary devices found intact at the site of the attempted arson and on the raid of a storage unit rented by Jeff Luers.

In a first trial, Jeff Luers was sentenced to 22 years and 8 months in prison, which was reduced to 10 years on appeal in 2008.[161] Craig Marshall was sentenced to 5 and a half years in a plea deal.[162]

5.35. Case against Marius Mason

Country: **United States (p. 40)**
Date: **1999 - 2010**
Technique used:

Informants (#1)

In 2008, Marius Mason was arrested and charged with several acts of arson and other vandalism claimed by the Earth Liberation Front (ELF) and the Animal Liberation Front (ALF)[163] from 1999 to 2003,[164] including a 1999 arson of an office associated with Genetically Modified Organism (GMO) research.

In a 2009 trial, Marius Mason was sentenced to 21 years and 10 months in prison, a sentence that was upheld on appeal in 2010.

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

[161]https://machorka.espivblogs.net/2014/03/07/interview-with-convicted-eco-terrorist-jeff-free-luers-2008

[162]https://nytimes.com/2002/04/07/magazine/from-tree-hugger-to-terrorist.html

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

[164]https://supportmariusmason.org/wp-content/uploads/2016/08/mason-plea-agreement-1.pdf

5.36. Case against Direct Action

Country: **Canada (p. 39)**
Date: **1982 - 1986**
Techniques used:

Covert house visit (#1)
Covert surveillance devices > Audio (#1)
Forensics > Linguistics (#1)
House raid (#1)
Mass surveillance > Civilian snitches (#1)
Physical surveillance > Aerial (#1)
Physical surveillance > Covert (#1)

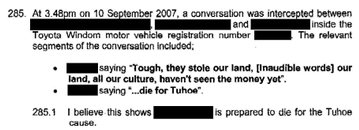
In 1983, five people were arrested and accused of being part of a group called Direct Action, which had carried out several actions in Canada in 1982, including the bombing of an electrical substation and the bombing of a factory belonging to the American defense contractor Litton Industries.[165] In the weeks prior to their arrest, they were planning to rob a guard of the cash handling company Brink's.

The main evidence in the case came from conversations recorded by microphones hidden in the group members' homes.

After several trials from 1983 to 1986,[166] the five people were sentenced to prison, with sentences ranging from ten years to life imprisonment. By 1990, all of them had been released on parole.

[165]https://archive.org/details/direct-action-memoirsofan-urban-guerrilla

[166]https://web.archive.org/web/20100715145801/http://uniset.ca/other/cs5/27CCC3d142.html



285. At 3.48pm on 10 September 2007, a conversation was intercepted between [redacted], [redacted] and [redacted] inside the Toyota Windom motor vehicle registration number [redacted]. The relevant segments of the conversation included;

- [redacted] saying "**Tough, they stole our land, [inaudible words] our land, all our culture, haven't seen the money yet**".
- [redacted] saying "**...die for Tuhoe**".

285.1 I believe this shows [redacted] is prepared to die for the Tuhoe cause.

Extract from the court document used to justify the raids, showing how the words "die for Tūhoe," taken out of context from a private conversation, were used to suggest that someone was "prepared to die for the Tūhoe cause" (personal information censored by the No Trace Project). Tūhoe is a Māori *iwi* (tribe) whose members were particularly targeted by the operation.

On October 15, 2007, approximately 60 raids targeting Māori indigenous activists, anarchists, and other activists took place across New Zealand as part of an operation called "Operation 8."[152] A few more raids took place in 2007 and 2008. Around 20 people were arrested and initially accused of participating in a terrorist group and organizing "quasi-military training camps" in remote rural areas. In 2007 the original accusations were dropped and most of the defendants were instead charged with possession of weapons and Molotov cocktails and, for some of them, participation in a criminal group. In 2011 the charges against most of the defendants were dropped and only four people remained charged.[153]

The operation started in 2006 when the police became aware of the "training camps."[154]

In a 2012 trial:

- Two people were sentenced to 2 years and 6 months in prison.[155]
- Two people were sentenced to 9 months of home detention.[156]

5.33. Scripta Manent

Country: **Italy (p. 39)**

[152]https://rebelpress.nz/wp-content/uploads/2021/03/Day_Raids_Came.pdf

[153]https://stuff.co.nz/national/5572235/Gun-charges-against-Urewera-accused-dropped

[154]https://putatara.net/2013/11/25/operation-8-the-evidence

[155]https://stuff.co.nz/national/crime/6976162/Protest-against-jailing-of-Urewera-pair

[156]https://web.archive.org/web/20250418153837/https://nzherald.co.nz/nz/urewera-pair-to-serve-time-at-home/XRXV2JUODXN54CK2YL7YQ44GPY

Date: **2003 - 2023**
Techniques used:

Forensics > DNA (#1)
Forensics > Handwriting analysis (#1)
Forensics > Linguistics (#1)
House raid (#1)
Targeted digital surveillance > Malware (#1)

In 2016, 32 house raids took place in different regions of Italy and several people were arrested as part of an operation called "Scripta Manent".[105] Up to 22 people were under investigation in this operation. They were accused of forming or participating in an *associazione sovversiva con finalità di terrorismo* (criminal association with the aim of terrorism), referring to attacks claimed by the *Federazione Anarchica Informale* (FAI, Informal Anarchist Federation) since 2003.[157] Some of them were accused of explosive attacks carried out between 2005 and 2016. Some of them were accused of *istigazione a delinquere* (incitement to commit a crime) for writing in the anarchist newspaper *Croce Nera Anarchica* (Anarchist Black Cross) or for running radical websites.

Scripta Manent combined the contents of several previous investigations.

A first trial took place in 2017-2019, an appeal in 2020, and two further verdicts in 2022[158] and 2023.[159] The final verdict is:

- Two people, Anna Beniamino and Alfredo Cospito, were sentenced to 17 years and 9 months and 23 years in prison, respectively.
- Eleven other people were sentenced to prison, with sentences ranging from 1 year and 9 months to 2 years and 6 months.
- The other people were acquitted.

5.34. Case against Jeff Luers

Country: **United States (p. 40)**
Date: **2000 - 2008**
Techniques used:

[157]https://tracesoffire.espivblogs.net/2016/09/13/italy-naples-september-carrion-operation-scripta-manent

[158]https://actforfree.noblogs.org/post/2022/07/10/italy-cassation-of-the-scripta-manent-trial

[159]https://actforfree.noblogs.org/post/2023/07/02/italy-anarchists-alfredo-cospito-and-anna-beniamino-have-been-sentenced-to-23-years-and-17-years-and-9-months

depending on your context, on the monitoring capabilities of the State, and on the VPN you use.

Therefore:

- You should use Tor for all your sensitive Internet activity, and as much of your non-sensitive Internet activity as possible.
- If you cannot use Tor for a given non-sensitive Internet activity (for example because you need to use a website that blocks Tor), you can use a VPN for it.
- You should not use the Internet without Tor or a VPN.

You can use both Tor and a VPN simultaneously by connecting to a VPN *before* Tor: this has several security benefits.[32] You should not connect to a VPN *after* Tor unless you really know what you are doing.[33]

Depending on your context, and in particular if you live in a country where few people use Tor or VPNs, using Tor or a VPN may attract unwanted attention or even make you a suspect in an investigation. To mitigate this, you can use the Internet outside your home on a connection that cannot be traced back to you.

Use end-to-end encrypted messaging applications

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

- Ideally, use peer-to-peer and **metadata-resistant (p. 18)** applications such as Cwtch[34] or Briar.[35] Otherwise, use metadata-resistant applications such as SimpleX[36] or Signal.[37]
- Email is not metadata-resistant and should be avoided if possible. If you must use email, use PGP encryption and register an address with a trusted service provider.[38]

[32]If you connect to a VPN before Tor, it is harder for the State to know that you are using Tor, and it can be harder for the State to obtain data about your Internet activity through advanced attacks such as traffic fingerprinting.

[33]https://privacyguides.org/en/advanced/tor-overview/#safely-connecting-to-tor

[34]https://cwtch.im

[35]https://briarproject.org

[36]https://simplex.chat

[37]https://signal.org

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

Do not use:

- Delta Chat or Matrix, as they are not sufficiently metadata-resistant.
- Telegram, as not all messages are end-to-end-encrypted.

See AnarSec's guide "Encrypted Messaging for Anarchists"[39] for recommendations of end-to-end messaging applications.

Back up your digital data

Back up your digital data regularly, especially data you really don't want to lose, such as your password manager database. Encrypt your backups with **Full Disk Encryption (p. 15)**. A typical practice is to have two backups:

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

The advantage of the on-site backup is that it has a more recent version of your data. The advantage of the off-site backup is that it cannot be seized in the event of a **house raid (#1)** against your home.

Store your devices in a tamper-evident way

If an adversary physically accesses one of your digital devices, they could tamper with it, making it unsafe to use. To detect when an adversary has physically accessed a device, you can use **tamper-evident preparation (p. 23)**.

Buy your devices anonymously

Buying digital devices anonymously (p. 6) has two advantages:

- If one of your digital devices is seized by an adversary, the adversary may recover information from the device using **digital forensics (#1)**. If you bought the device anonymously, the adversary may not be able to link the device, and thus the information they recovered, to you.
- If you buy a digital device in a way that doesn't give you immediate access to the device (e.g. if you order a laptop online), buying anonymously can prevent an

[39]https://anarsec.guide/posts/e2ee

adversary that is targeting you from tampering with the device before you gain access to it (e.g. between the purchase and the delivery of the laptop).

If necessary, physically destroy your storage devices

If you want to ensure that an adversary can never access the data stored on a storage device (e.g. a laptop's hard drive, a USB stick, a SD card), the only solution is to physically destroy the storage device. This is because:

- Even if the storage device is encrypted with **Full Disk Encryption (p. 15)** using a strong password, an adversary could **bypass the encryption (#1)**.
- Modern storage devices can store a hidden copy of their data in *spare memory cells*,[40] so overwriting the entire device is not sufficient.

To physically destroy a storage device:

- First, reformat and overwrite the entire storage device as an additional safety precaution.
- Then, use a high-quality household blender or an angle grinder to shred it into pieces, ideally less than two millimeters in size.

Other best practices

- Phishing is when an adversary tricks you into revealing sensitive information or installing **malware (#1)** on one of your digital devices. To mitigate this, do not open files or click links sent to you by people you don't trust. See AnarSec's "Phishing Awareness" section[41] on the measures you can take against phishing.
- **Doxing (#1)** is when an adversary publishes your personal information without your consent. See Doxcare: Prevention and Aftercare for Those Targeted by Doxxing and Political Harassment[42] on the measures you can take against doxing.

[40] https://tails.net/doc/encryption_and_privacy/secure_deletion/index.en.html
[41] https://anarsec.guide/posts/tails-best/#phishing-awareness
[42] https://notrace.how/resources/#doxcare

4.15. DNA minimization protocols

Technique addressed by this mitigation:
Forensics > DNA (#1)

DNA minimization protocols allow you to manipulate objects while minimizing the amount of **DNA (#1)** you leave on them. Some protocols focus on never leaving DNA traces on an object in the first place. Other protocols focus on removing DNA traces from an object by chemically destroying DNA molecules.

DNA minimization protocols may involve:

- Purchasing an object in individual plastic packaging so that you don't risk leaving DNA on it until you open the packaging.
- Manipulating an object while wearing a new pair of non-permeable gloves (e.g. dish washing gloves) so that there are no DNA traces on the outside of the gloves that could be transferred to the object.
- Storing an object in a new, non-permeable garbage bag so that DNA from the environment doesn't contaminate the object during storage.
- Destroying DNA molecules with sodium hypochlorite, which is present in adequate concentrations in some brands of bleach.

See "Dna You Say? Burn Everything to Burn Longer: A Guide to Leaving No Traces"[43] for protocol suggestions, and the "DNA" topic.[44]

4.16. Encryption

Techniques addressed by this mitigation:

[43] https://notrace.how/resources/#dna-you-say
[44] https://notrace.how/resources/#topic=dna

After a trial in 2014, two people were sentenced to 16 years in prison.[143] After another trial in 2014[144] and an appeal in 2016,[145] the other two were sentenced to 9 and 11 years in prison, respectively.

5.30. Case against Amos Mbedzi

Country: **Eswatini (p. 39)**
Date: **2008 - 2012**
Techniques used:
Forensics > DNA (#1)
Mass surveillance > Civilian snitches (#1)
Physical violence (#1)
Service provider collaboration > Mobile network operators (#1)

In 2008, Amos Mbedzi took part in an attempt to bomb a bridge in Eswatini with an explosive device.[146] Mbedzi and two of his comrades were under the bridge preparing the device when it exploded prematurely, severely wounding Mbedzi and killing his two comrades, without damaging the bridge.[147] A passing car brought Mbedzi to a hospital, where he was arrested one hour later. Mbedzi was charged with sedition for the bombing attempt and with murder for the deaths of his comrades.

In a 2012 trial, Mbedzi was convicted of sedition and murder and sentenced to 25 years in prison. He died in prison in 2022.[148]

5.31. Mauvaises intentions

Country: **France (p. 39)**
Date: **2006 - 2012**
Techniques used:
Forensics > Arson (#1)
Forensics > DNA (#1)
Network mapping (#1)
Physical surveillance > Overt (#1)
Service provider collaboration > Mobile network operators (#1)

In 2008, six people were arrested and charged with preparation of terrorist acts, possession or manufacture of explosive or incendiary devices, and arson or attempted arson—including an attempted arson of an electrical cabinet in 2006 and an attempted arson of a police tow truck in 2007.[149] This operation was documented by comrades in a series of zines entitled "Mauvaises intentions".[150]

After a trial in 2012, five people were sentenced to between one and three years in prison.[151]

5.32. Operation 8

Country: **New Zealand (p. 39)**
Date: **2006 - 2012**
Techniques used:
Biased interpretation of evidence (#1)
Covert surveillance devices > Audio (#1)
Covert surveillance devices > Video (#1)
Forensics > Gait recognition (#1)
House raid (#1)
Informants (#1)
Network mapping (#1)
Open-source intelligence (#1)
Physical surveillance > Aerial (#1)
Physical surveillance > Covert (#1)
Roadblocks (#1)
Service provider collaboration > Mobile network operators (#1)
Service provider collaboration > Other (#1)

[142] https://machorka.espivblogs.net/2016/02/26/appeal-trial-for-the-double-bank-robbery-velvendo-case-greece
[143] https://machorka.espivblogs.net/2014/10/02/announcement-of-sentences-in-the-velvedo-double-robbery-case-11014-athens
[144] https://abcsolidaritycell.espivblogs.net/archives/tag/g-naxakis
[145] https://anarhija.info/library/grecia-l-ultimo-aggiornamento-sul-processo-d-appello-per-rapina-a-pirgetos-con-anarchic-en
[146] https://web.archive.org/web/20120922005905/http://www.bdlive.co.za/world/africa/2012/09/18/sa-man-gets-85-years-for-plot-on-mswati
[147] https://notrace.how/documentation/case-against-amos-mbedzi-case-file.pdf
[148] https://peoplesdispatch.org/2022/06/08/south-african-communist-amos-mbedzi-who-fought-apartheid-dies-a-martyr-for-liberation-of-swaziland
[149] https://infokiosques.net/spip.php?article597
[150] https://notrace.how/resources/#mauvaises-intentions
[151] https://juralib.noblogs.org/2012/06/25/mauvaises-intentions-paris-rendu-du-proces-antiterroriste-de-mai-2012

Techniques used:

Forensics > Digital (#1)
House raid (#1)
Mass surveillance > Video surveillance (#1)
Open-source intelligence (#1)
Police patrols (#1)
Service provider collaboration > Mobile network operators (#1)
Service provider collaboration > Other (#1)

In 2014, eight alleged members or sympathizers of the Swedish anti-fascist organization Revolutionära fronten (*Revolutionary Front*) were accused of committing various offenses in 2013.[85] In particular:

- Five defendants were accused of beating two people near a demonstration organized by a neo-Nazi political party in Stockholm.
- Four defendants were accused of visiting a fascist's house at night, hitting the door with an ax and painting threatening graffiti on the facade.
- One defendant was accused of possessing Molotov cocktails.

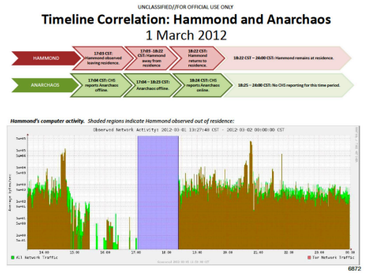
In a 2014 trial:

- Five defendants were sentenced to prison, with sentences ranging from 1 year and 2 months to 2 years and 4 months.
- Two defendants were sentenced to fines.
- One defendant was acquitted.

5.28. 2011-2013 case against Jeremy Hammond

Country: **United States (p. 40)**
Date: **2011 - 2013**
Techniques used:

Informants (#1)
Mass surveillance > Police files (#1)
Physical surveillance > Covert (#1)
Targeted digital surveillance > Authentication bypass (#1)
Targeted digital surveillance > Network forensics (#1)



Timeline established by investigators, showing a correlation between the times when Jeremy Hammond was physically present at his home, the times when his online persona (*anarchaos*) was reported as being online by an informant, and the times when the network traffic of the router he was using showed usage of the Tor network.

In March 2012, Jeremy Hammond's home was raided and he was arrested for his involvement in a December 2011 cyber-attack on Stratfor, a private intelligence firm.[137]

The case was in a large part based on information provided to investigators by Sabu, an associate of Jeremy Hammond who became an informant.

In a 2013 trial, Jeremy Hammond was sentenced to 10 years in prison.[138]

5.29. Nea Filadelphia case

Country: **Greece (p. 39)**
Date: **2011 - 2016**
Techniques used:

Forensics > DNA (#1)
Physical surveillance > Covert (#1)

In 2013, several people were arrested in Nea Filadelphia, a suburb of Athens.[139] Four of them were accused of carrying out bank robberies[140] in 2011[141] and 2013.[142]

[137] https://rollingstone.com/culture/culture-news/the-rise-and-fall-of-jeremy-hammond-enemy-of-the-state-183599
[138] https://apnews.com/general-news-1632c936e6d74d42aa465878d144aaae
[139] https://web.archive.org/web/20201027031238/http://actforfree.nostate.net/?p=15472
[140] https://machorka.espivblogs.net/2013/11/06/concerning-the-arrests-of-comrades-in-nea-philadelphia-on-304-athens
[141] https://abcsolidaritycell.espivblogs.net/archives/130

Forensics > Digital (#1)
Mass surveillance > Mass digital surveillance (#1)
Service provider collaboration > Mobile network operators (#1)
Service provider collaboration > Other (#1)
Targeted digital surveillance > IMSI-catcher (#1)
Targeted digital surveillance > Malware (#1)
Targeted digital surveillance > Network forensics (#1)

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

You can encrypt "at rest" data on a digital device by enabling Full Disk Encryption (FDE) on the device with a **strong password (p. 12)**. When the device is turned off, its data is encrypted; when you turn it on and enter the decryption key, its data is decrypted until it is turned off. If a device with FDE enabled is seized by an adversary during an arrest, **house raid (#1)**, or **covert house visit (#1)** while it is turned off, the adversary will not be able to access its data (unless they **bypass its authentication (#1)**).

You can encrypt "in motion" data by using Tor[31] or a Virtual Private Network (VPN) for your Internet activity, and by using **end-to-end encrypted messaging applications (p. 12)** for your digital communications. Encrypting "in motion" data can prevent an adversary from monitoring your digital activity.

Encryption should be considered a harm-reduction measure, not a panacea. You should not use digital devices for incriminating activities unless it's unavoidable, and you should have all your incriminating conversations **outdoors and without electronic devices (p. 19)**.

4.17. Fake ID

Techniques addressed by this mitigation:

ID checks (#1)
Network mapping (#1)

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

A fake ID can consist of:

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

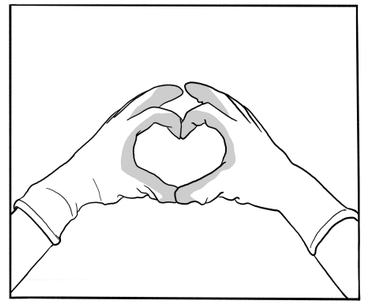
You can use a fake ID:

- To mitigate **network mapping (#1)** or avoid arrest in the event of an **ID check (#1)**.
- To establish a **safe house (p. 21)**.
- To take the path of **clandestinity (p. 11)**.

4.18. Gloves

Techniques addressed by this mitigation:

Forensics > DNA (#1)
Forensics > Fingerprints (#1)



Gloves can prevent you from leaving fingerprints and DNA on surfaces you touch, and can hide your hand characteristics.

Fingerprints and DNA

To avoid leaving fingerprints and DNA on surfaces you touch, use the right kind of gloves:

- Use non-permeable, thick latex or rubber gloves.
- Do not use thin gloves (such as thin latex or rubber gloves) because your fingerprints can pass through them.
- Do not use leather gloves because they can leave their own unique prints on surfaces you touch (called glove prints[45]).

- Do not use work gloves by themselves because they are generally permeable, and can let your sweat (and therefore your DNA) out.

And take appropriate precautions:

- Make sure that your DNA is not already on the outside of the gloves, because it would be transferred from the gloves to any surface you touch. To ensure this, you can use a new pair of gloves that come in airtight packaging.
- Do not leave your DNA on the outside of the gloves when you put them on. To ensure this, you must put them on without touching the outside of the gloves.[46]
- While wearing the gloves, do not touch your skin or any surface that might contain your DNA, because the DNA would be transferred from the surface to the gloves and from there to any surface you touch.

You can wear multiple pairs of gloves on top of each other. For example, wearing work gloves on top of thick latex or rubber gloves gives you both the sturdiness of the work gloves and the non-permeability of the thick latex or rubber gloves.

If you wear gloves to avoid leaving DNA on surfaces you touch, you will also want to avoid leaving DNA in other ways (e.g., skin flakes or hair falling off your body). For more information, see the related mitigation **DNA minimization protocols (p. 15)**.

Hand characteristics

To hide your hand characteristics such as skin color or tattoos, wear gloves that fully cover your skin. See the related mitigation **Anonymous dress (p. 5)**.

Additional considerations

When using gloves, you should be aware that:

- You can leave fingerprints on the inside of gloves you wear, depending on their material.
- You leave DNA on the inside of gloves you wear.
- If you wear gloves during an action, traces from the action site (e.g., traces of accelerant) may be deposited on the gloves, and traces from the gloves (e.g., textile fibers) may be deposited at the action site. These traces could be used to link the gloves to the action site.

For all these reasons, if you need to use gloves during an action, you should use new gloves dedicated to the action and dispose of them afterward.

See also

- The "Fingerprints" topic.[47]
- Handschuhe[48] (in German).

4.19. Masking your writing style

Technique addressed by this mitigation:
Forensics > Linguistics (#1)

Masking your writing style is the practice of altering the way you write to counter author identification by **forensic linguistics (#1)**.

For example:

- You can write with brevity and intent.
- Before publishing a text, you can check it for spelling and grammatical errors to ensure that it does not contain any unique errors that could be traced back to you.
- To identify someone as the author of a text, an adversary can look for samples of that person's writing to use for comparison. To mitigate this, you can avoid keeping unencrypted samples of your writing at home that might be found in a **house raid (#1)** or **covert house visit (#1)**, and generally avoid publishing texts in your name throughout your life.

See Counteracting Forensic Linguistics[49] and Who wrote that?[50]

[45] https://en.wikipedia.org/wiki/Glove_prints

[46] To do this, pinch the inside of the left glove with your right hand and put your left hand into it (if you're right-handed, otherwise reverse), then pinch the outside of the right glove with your left gloved hand and put your right hand into it.

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

[48] https://web.archive.org/web/20250615110720/https://militanz.blackblogs.org/163-2

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

[50] https://notrace.how/resources/#who-wrote

management of a migrant detention center.[125] In July 2020, Carla, who had been on the run since the first arrests, was arrested in France and extradited to Italy.

After a trial in 2021[126]–2023, several people were sentenced to prison, with sentences ranging from 1 year to 4 years and 2 months.[127]

5.25. Fenix

Country: **Czech Republic (p. 39)**
Date: **2014 - 2018**
Techniques used:
Detection dogs (#1)
Infiltrators (#1)
Mass surveillance > Civilian snitches (#1)

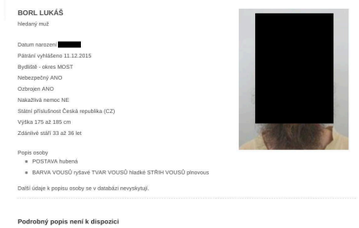

BORL LUKÁŠ
Nedaný muž
Datum narození: [redacted]
Pátrání vyhlášeno 11.12.2015
Bydliště - okres MOST
Nebezpečný ANO
Ozbrojen ANO
Nakažlivá nemoc NE
Státní příslušnost Česká republika (CZ)
Výška 175 až 185 cm
Zdánlivě stáří 33 až 36 let
Popis osoby
- POSTAVA hubená
- BARVA VOUSŮ rýšavé TVAR VOUSŮ hladké STŘIH VOUSŮ plnovous
Další údaje k popisu osoby se v databázi nevyskytují.
Podrobný popis není k dispozici

Photo and personal information of Lukáš Borl published on the national police website (date of birth and picture censored by the No Trace Project).[128]

In 2015, house raids took place and several people were charged with crimes as part of an operation called "Fenix".[129] Some of them were accused of the arson of a police car in 2014.[130] Some of them were accused of having planned to attack a train.

Some of the people were detained for several months before being released. One of them, Lukáš Borl, entered clandestinity to avoid arrest and stayed in clandestinity for several months before being arrested and detained for several months.[131]

In a 2017 trial, the people were acquitted. In a 2018 appeal, the acquittals were confirmed.[132]

5.26. 2013 case against Mónica and Francisco

Country: **Spain (p. 40)**
Date: **2013 - 2017**
Techniques used:
Forensics > Facial recognition (#1)
House raid (#1)
Mass surveillance > Video surveillance (#1)

In 2013, Mónica Caballero and Francisco Solar were arrested in Spain, accused of placing an explosive device in a church.[133] The device exploded, causing material damages and slightly injuring one person.

In a trial in 2016, Mónica and Francisco were each sentenced to 12 years in prison.[134] In a 2016 appeal, both of their sentences were reduced to 4 years and 6 months.[135] In 2017, Mónica and Francisco were expelled to Chile, their country of origin.[136]

5.27. Case against Revolutionära fronten

Country: **Sweden (p. 40)**
Date: **2013 - 2014**

[125] https://web.archive.org/web/20200918130026/https://roundrobin.info/2019/12/verona-una-perquisizione-e-un-arresto

[126] https://web.archive.org/web/20211012182815/https://roundrobin.info/2021/10/op-scintilla-inizio-del-processo-e-volantino

[127] https://ilrovescio.info/2023/01/18/torino-sentenza-di-primo-grado-del-processo-scintilla

[128] https://web.archive.org/web/20160314103136/http://aplikace.policie.cz/patrani-osoby/PersonDetail.aspx?person_id=13081211150011

[129] https://antifenix.noblogs.org/post/2017/11/10/repressions-in-so-called-czech-republic-timeline-a2-poster

[130] https://antifenix.noblogs.org/post/2015/06/03/interview-with-an-activist-detained-during-operation-fenix

[131] https://antifenix.noblogs.org/post/2016/10/19/lukas-borl-statement-about-his-arrest

[132] https://antifenix.noblogs.org/post/2018/03/30/vrchni-soud-potvrdil-osvobozujici-verdikt-mestskeho-soudu-high-court-in-prague-confirmed-acquittance-of-all-defendants

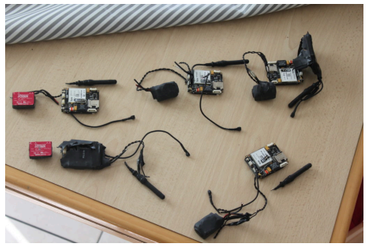
[133] https://notrace.how/documentation/monica-and-francisco-2013-case-file.pdf

[134] https://alasbarricadas.org/noticias/node/36054

[135] https://es-contrainfo.espiv.net/2016/12/17/estado-espanol-reducida-a-4-anos-y-medio-de-prision-la-sentencia-contra-lxs-companerxs-francisco-solar-y-monica-caballero

[136] https://es-contrainfo.espiv.net/2017/03/10/estado-espanol-comunicado-de-lxs-companerxs-anarquistas-monica-caballero-y-francisco-solar

House raid (#1)
Physical violence (#1)



Surveillance devices found in a house after the operation.[119]

In February 2019, 50 house raids took place, mainly in Trentino, and seven people were arrested as part of an operation called "Renata".[105] More people were arrested in May 2019. The people arrested were accused of participating in an *associazione sovversiva* (criminal association) and carrying out various arson and explosive attacks between 2016 and 2018, including an explosive attack on the headquarters of the right-wing political party Lega Nord in Treviso. Some people were also accused of forging documents.

In a trial in December 2019, several people were sentenced to prison, with sentences ranging from one year and nine months to two years and six months.

5.23. Warsaw 3

Country: **Poland (p. 39)**
Date: **2016 - 2017**
Techniques used:

Interrogation techniques (#1)
Physical violence (#1)

In 2016, three people were arrested[120] in the parking lot of a police station in Warsaw.[121] They were accused of attempting to set fire to police cars.

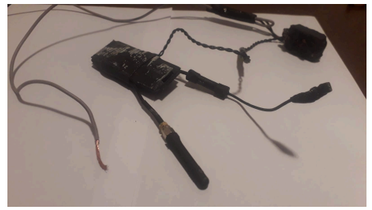
The people were detained for 4 months before being released.

In a 2017 trial, the people were sentenced to 3 months in prison (which they had already served), a fine, and 24 months of community service.

5.24. Scintilla

Country: **Italy (p. 39)**
Date: **2015 - 2023**
Techniques used:

Covert surveillance devices > Audio (#1)
Door knocks (#1)
Forensics > DNA (#1)
Forensics > Gait recognition (#1)
International cooperation (#1)



Microphones found in a house[122] that were used to surveil the defendants.

In February 2019, the *Asilo Occupato* squat in Turin was evicted and six people were arrested—a seventh person, Carla, went on the run—as part of an operation called "Scintilla".[105] Some of them were accused of carrying out several arson and explosive attacks on migrant detention centers and other targets between 2015 and 2018.[123] Some of them were accused of publishing a zine called "I cieli bruciano" ("The skies are burning") which contained information about entities responsible for the management and maintenance of migrant detention centers.

In May 2019, another person, Boba, was arrested and accused of setting fire to a prison building with a flare during a gathering in front of the prison where the other people were detained.[124] In November 2019, another person, Peppe, was arrested and accused of sending a parcel bomb in 2016 to a company involved in the

[119] https://notrace.how/earsandeyes/#trento-2019-03
[120] https://wawa3.noblogs.org/post/2016/06/21/chronology-eng
[121] https://wawa3.noblogs.org/post/2017/05/24/olsen-gang-replies-statements-of-warsaw-three-en
[122] https://notrace.how/earsandeyes/#torino-2019-03
[123] https://attaque.noblogs.org/post/2020/08/06/saint-etienne-arrestation-de-carla-recherchee-dans-le-cadre-de-loperation-scintilla
[124] https://macerie.org/index.php/2019/05/23/incendio-al-carcere-boba-arrestato

4.20. Metadata erasure and resistance

Technique addressed by this mitigation:
Forensics > Digital (#1)

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

Examples of metadata

Examples of metadata include:

- An image file can embed information about when it was taken and the camera or phone that took it.
- A PDF file can embed information about the computer that created it.
- An email embeds the email address that sent it and the email address that received it.
- A printed document often has an invisible watermark[51] that identifies the make and model of the printer that printed it.

Metadata erasure

For digital files, metadata erasure can be accomplished using MAT2[52] or similar software. Some **security-oriented operating systems (p. 12)** include metadata erasure tools by default.

Metadata resistance

Examples of metadata resistance include:

- Using a dedicated operating system (e.g. a Tails[15] stick) to create or modify digital files so that information about the operating system you normally use is not embedded in the metadata of the files.
- Using **metadata-resistant messaging applications (p. 12)**.

[51] https://eff.org/issues/printers
[52] https://github.com/tpet/mat2

See also

See AnarSec's guide "Remove Identifying Metadata From Files"[53] on how to remove metadata from digital files.

4.21. Need-to-know principle

Techniques addressed by this mitigation:
Biased interpretation of evidence (#1)
Infiltrators (#1)
Informants (#1)
Network mapping (#1)
Physical violence (#1)

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

In relation to a planned or past action, the need-to-know principle should be applied in the following ways:

- People not involved in the action should not speculate about who is involved.
- People involved in the action should not disclose their involvement to people who are not involved.
- People who have a specific and limited role in the action may not need to know who else is involved other than the person with whom they are communicating directly.

In addition, everyone should stop any violation of the need-to-know principle in conversations. For example, if you hear people talking about their involvement in an action or speculating about the involvement of others, tell them to stop.

When multiple groups of people participate in an action, a coordinating structure that embodies the need-to-know principle is the "spokes council". In this structure, one or two people from each group are designated to participate in the spokes council, where they meet with the designated people from the other groups. In this way, the groups can coordinate through the spokes council without anyone having to know everyone involved. However, this structure runs the risk of creating "choke

[53] https://anarsec.guide/posts/metadata

points" of coordination—if one person is the only bridge between two groups, this can create a gate-keeping dynamic, as well as make coordination impossible if that person is arrested by an adversary.

See also:

- Secrets And Lies[54] about the effects that secrecy can have on an individual and collective level.
- The "Security culture" topic.[55]

4.22. Network map exercise

Techniques addressed by this mitigation:

Infiltrators (#1)
Informants (#1)
Network mapping (#1)
Targeted digital surveillance > Physical access (#1)

A network map exercise consists of creating a graphical representation of the links between you and the people in your network in order to critically examine those links. This exercise is designed to sharpen your ability to make informed and critical choices about the people you associate with, with the ultimate goal of making your network more resilient to **infiltration (#1)** attempts.

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

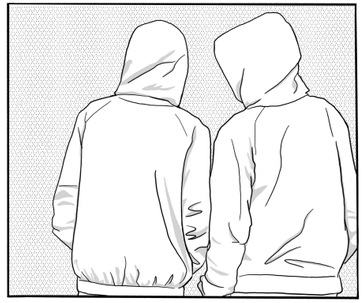
For instructions on how to do this, see Stop hunting sheep: a guide to creating safer networks.[56] Such a network map would be invaluable to an adversary—it is essentially what they construct during **network mapping (#1)**—so it should be burned immediately after use.

[54]https://notrace.how/resources/#secrets-lies
[55]https://notrace.how/resources/#topic=security-culture
[56]https://notrace.how/resources/#stop-hunting

4.23. Outdoor and device-free conversations

Techniques addressed by this mitigation:

Covert surveillance devices > Audio (#1)
Mass surveillance > Video surveillance (#1)



Outdoor and device-free conversations is the practice of conducting sensitive or incriminating conversations outdoors and without electronic devices, to ensure that they are not overheard by an adversary.

Outdoor and device-free conversations are necessary because:

- Indoor spaces, including cars can contain **covert surveillance devices (#1)**.
- Electronic devices can be infected with **malware (#1)** that can turn them into covert microphones.

Outdoor conversations can be recorded with covert microphones or long-range parabolic microphones during a **physical surveillance (#1)** operation (with ranges of up to 300 meters). For example, in Italy in 2019[57] a microphone was hidden in a fake stone in front of a prison where gatherings were often held. For this reason, you should conduct outdoor conversations while walking, or for larger group conversations where it would be difficult to move, conduct them in spaces that change regularly and are difficult to place under audio surveillance.

During device-free conversations, you should not turn off your phone, remove its batteries, or place it in a Faraday bag, as this generates **metadata (p. 18)** about who is having sensitive conversations, when, and where. Instead, leave your phone at home. Also, a Faraday bag does not prevent audio from being captured, only from

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

5.19. Network

Country: **Russia (p. 40)**
Date: **2017 - 2020**
Technique used:

Physical violence (#1)

In late 2017 and early 2018, about ten people were arrested in Penza and Saint Petersburg[110] and accused of being part of an underground organization called "Network" that was allegedly planning attacks in anticipation of the 2018 Russian presidential elections and the FIFA World Cup.[111] Some were also accused of attempting to sell large quantities of drugs. Most of them were tortured in the early stages of their detention by the Russian Federal Security Service (FSB).

The initial arrests that launched the investigation were made because most of the defendants from Penza were involved in the drug business.[112]

After two trials in 2020, seven alleged members of the "Network" organization in Penza were sentenced to prison terms ranging from 6 to 18 years,[113] and two alleged members in Saint Petersburg were sentenced to 5 and a half and 7 years in prison, respectively.[114]

5.20. Panico

Country: **Italy (p. 39)**
Date: **2016 - 2023**
Technique used:

Forensics > DNA (#1)

In 2017, house raids took place in Florence and several people were arrested as part of an operation called "Panico".[105] Up to 35 people were charged in this operation.[115] Some were accused of carrying out an explosive attack on a fascist bookshop in 2017 and an arson attack on a police station in 2016. Others were accused of various other actions.

After a trial in 2019, an appeal in 2021[116] and a ruling by the Court of Cassation in 2023,[117] two people were sentenced to 8 years in prison, while others received sentences ranging from a few months to three and a half years.

5.21. Prometeo

Country: **Italy (p. 39)**
Date: **2016 - 2021**
Techniques used:

Evidence fabrication (#1)
Forensics > DNA (#1)
Mass surveillance > Video surveillance (#1)

In 2019, three people were arrested as part of an operation called "Prometeo".[105] They were accused of sending parcel bombs to prosecutors and a director of the prison administration in 2017. One of them was also accused of carrying out an arson attack on an Automated Teller Machine (ATM) in 2016.

In 2021, the person accused of the ATM arson was sentenced to 5 years in prison and the other people were acquitted (for lack of evidence[118]) for the parcel bombs, although one of them had spent two and a half years in prison before being acquitted.

5.22. Renata

Country: **Italy (p. 39)**
Date: **2016 - 2019**
Techniques used:

Covert surveillance devices > Audio (#1)
Forensics > DNA (#1)

[110]https://web.archive.org/web/20210724133854/https://a2day.net/network-underground
[111]https://amnesty.org/en/wp-content/uploads/2021/05/EUR4696252018ENGLISH.pdf
[112]https://web.archive.org/web/20210724130151/https://a2day.net/the-dark-side-of-the-network-case
[113]https://therussianreader.com/2020/02/10/network-penza-sentences
[114]https://anarchistsworldwide.noblogs.org/post/2020/06/23/saint-petersburg-russia-we-can-dance-if-we-want-to-sentencing-of-the-network-case-defendants
[115]https://insuscettibiledirawedimento.noblogs.org/post/2019/07/18/it-en-italia-richieste-di-condanna-al-processo-per-loperazione-panico
[116]https://ilrovescio.info/2021/05/05/sentenza-dappello-processo-panico
[117]https://lanemesi.noblogs.org/post/2023/07/15/sentenza-di-cassazione-del-processo-panico-14-luglio-2023
[118]https://actforfree.noblogs.org/post/2021/10/06/italy-op-prometeo-beppe-robert-and-nat-acquitted

To find and arrest Stecco, investigators placed a large number of people under surveillance whom they believed could lead them to him.

In October 2023, Stecco was arrested after nearly two years on the run.

5.17. Bialystok

Country: **Italy (p. 39)**
Date: **2017 - 2022**
Techniques used:

Forensics > Gait recognition (#1)
International cooperation (#1)

In June 2020, house raids took place in the *Bencivenga Occupato* squat in Rome and other places, and seven people were arrested in Italy, Spain and France as part of an operation called "Bialystok".[105] They were accused of participating in an *associazione sovversiva* (criminal association) and of various minor offenses related to initiatives in solidarity with people accused in the **Panico operation (p. 32)**. Two of them were accused of carrying out an explosive attack on a police station in 2017 and an arson attack on cars linked to ENI (an Italian multinational oil and gas company) in 2019, respectively.

After a trial in 2022, some people were acquitted and some were sentenced to prison, with sentences ranging from 45 days to one year.[106]

5.18. Bure criminal association case

Country: **France (p. 39)**
Date: **2017 - 2025**
Techniques used:

Covert surveillance devices > Location (#1)
Detection dogs (#1)
Forensics > Arson (#1)
Forensics > DNA (#1)
Forensics > Digital (#1)
Forensics > Fingerprints (#1)
House raid (#1)
International cooperation (#1)
Mass surveillance > Police files (#1)
Mass surveillance > Video surveillance (#1)
Open-source intelligence (#1)
Physical surveillance > Covert (#1)
Service provider collaboration > Mobile network operators (#1)
Service provider collaboration > Other (#1)
Targeted digital surveillance > Authentication bypass (#1)
Targeted digital surveillance > IMSI-catcher (#1)

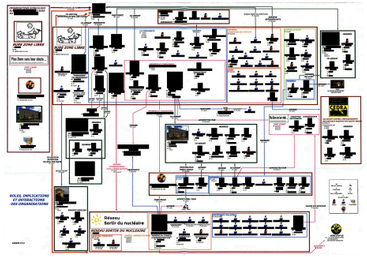


Diagram of the organizations fighting against Cigéo and their members, made by investigators (personal information censored by the No Trace Project).

In 2017 and 2018, around 20 house raids took place in France and around 10 people were arrested and accused of various crimes related to the struggle against Cigéo, a project to build a radioactive waste disposal facility in Bure, France.[107] Some of the people were accused of organizing or participating in demonstrations in which people attacked police forces and buildings associated with Cigéo, including a demonstration on June 21, 2017, in which a small fire broke out in a building while civilians were inside. Some of the people were charged with possession of explosive materials. Some were accused of being part of an *association de malfaiteurs* (criminal association).[108]

After a trial in 2021, an appeal in 2023, and another appeal in 2025,[109] everyone was acquitted.

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

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

[107] https://burebure.info/repression

[108] https://noussommestousdesmalfaiteurs.noblogs.org/antecedents-familiaux

[109] https://noussommestousdesmalfaiteurs.noblogs.org/relaxe-generale

being transmitted, which could happen when the phone later reconnects to the network.

See the "Security culture" topic.[55]

4.24. Physical intrusion detection

Techniques addressed by this mitigation:

Covert house visit (#1)
Covert surveillance devices > Audio (#1)
Covert surveillance devices > Location (#1)
Covert surveillance devices > Video (#1)
Evidence fabrication (#1)
Targeted digital surveillance > Physical access (#1)

Physical intrusion detection is the process of detecting when an adversary enters or attempts to enter a space, for example for a **covert house visit (#1)**. You can do this by making sure there is always someone in the space who would notice if an adversary tried to enter, or by monitoring the space with a video surveillance system.

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

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

4.25. Preparing for house raids

Techniques addressed by this mitigation:

Covert house visit (#1)
House raid (#1)

Preparing for house raids is the process of taking precautionary measures to minimize the impact of a potential **house raid (#1)** or **covert house visit (#1)**.

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

- You should encrypt all digital devices with **Full Disk Encryption (p. 15)**, and turn them off overnight or when you are away for the encryption to be effective.
- You should store materials used for actions that can appear to have a "legitimate" purpose where they belong and not together (gloves with cleaning supplies, etc.)
- You should store materials used in actions that have no "legitimate" purpose in a **stash spot or safe house (p. 21)**, or at worst, let them pass through your home for a very limited time. In most contexts, we do not think it makes sense to avoid keeping anarchist literature at home, but you should avoid keeping particularly sketchy guides.

In addition, to detect if an adversary has **physically accessed (#1)** an electronic device during a covert house visit, you can use **tamper-evident preparation (p. 23)**.

4.26. Preparing for repression

Techniques addressed by this mitigation:

House raid (#1)
Physical violence (#1)

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

Examples of practical preparation include:

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

State can use drug charges to put pressure on you for the crimes they are really interested in.

Examples of psychological preparation include:

- Talking with comrades who have been the target of repression about their experiences, including their experiences of imprisonment.
- An experience described in Claudio Lavazza's autobiography[58] where he secluded himself in a house in the mountains for a month to prepare for the possibility of his imprisonment.

4.27. Prisoner support

Technique addressed by this mitigation:
Informants (#1)

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

Common prisoner support initiatives include:

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

4.28. Reconnaissance

Techniques addressed by this mitigation:
Alarm systems (#1)
Guards (#1)
Mass surveillance > Video surveillance (#1)
Police patrols (#1)

Reconnaissance is the gathering of information about the target of an action. It precedes **action planning (p. 10)**. It can be done either physically (e.g., by traveling to the action site to inspect it) or digitally (e.g., by researching the target on the web). You should take into account the techniques an adversary may use against you during reconnaissance as much as you take them into account during the action itself.

Physical reconnaissance

Examples of physical reconnaissance include:

- Inspecting possible routes to and from the action site to evaluate which route you might take. For example, a good route may have minimal **surveillance camera (#1)** coverage and a suitable place to change clothing before the action.
- Inspecting the action site itself, looking for surveillance cameras, **guards (#1)**, **alarm systems (#1)** and opportunities to attack the target.

When conducting physical reconnaissance, you can:

- Practice **anti-surveillance (p. 7)** to counter the risk of physical surveillance.
- **Dress anonymously (p. 5)** to counter the risk of being observed or recorded.

Digital reconnaissance

Examples of digital reconnaissance include:

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

When conducting digital reconnaissance, you should follow **digital best practices (p. 12)**.

4.29. Stash spot or safe house

Techniques addressed by this mitigation:
Covert house visit (#1)
Covert surveillance devices > Video (#1)
Forensics > Ballistics (#1)
Forensics > Trace evidence (#1)
House raid (#1)

Stash spots and safe houses are two ways to store incriminating materials. If incriminating materials are stored in a stash spot or safe house instead of in your home, they won't be found by an adversary in the event of a **house raid (#1)** or a **covert visit (#1)** of your residence. A stash spot is a hidden place, often outdoors, that is

[58] https://notrace.how/documentation/claudio-lavazza-seclusion-experience.pdf

5.15. December 8 case

Country: **France (p. 39)**
Date: **2018 - ?**
Techniques used:
Biased interpretation of evidence (#1)
Covert surveillance devices > Audio (#1)
Covert surveillance devices > Location (#1)
Covert surveillance devices > Video (#1)
Evidence fabrication (#1)
Forensics > Trace evidence (#1)
House raid (#1)
Interrogation techniques (#1)
Physical surveillance > Covert (#1)
Service provider collaboration > Mobile network operators (#1)
Targeted digital surveillance > IMSI-catcher (#1)

On December 8, 2020 several raids took place across the country and nine people were arrested.[98] One person among them, *Libre Flot*, was under surveillance by French intelligence services since 2018, when he came back to France after spending a few months in Rojava.[99] The other eight people didn't all know each other but all knew Libre Flot. After the arrests, seven people (including Libre Flot) were accused of being part of a terrorist association that was planning attacks against French institutions.

To identify the phone numbers used by some of the defendants, investigators analyzed correlations between different sets of data, obtained through:[100]

- Real-time geolocation of phones, through the **collaboration of mobile network operators (#1)**.
- **IMSI-catchers (#1)**.
- **Covert location surveillance devices (#1)**.
- **Physical surveillance (#1)** operations.

Some of the defendants spent time in pre-trial detention, with durations ranging from 4 to 16 months. Libre Flot was detained in isolation for 16 months.

In a 2023 trial:[101]

- Seven defendants were sentenced to prison, with sentences ranging from 2 to 5 years (parts of the sentences were suspended prison sentences).
- Among them, six were sentenced to registration in the *Fichier des Auteurs d'Infractions Terroristes* (FIJAIT, Terrorist offenders index): for 10 years, they will have to check in every three months at a police station and to notify authorities two weeks before traveling abroad, under penalty of 2 years in prison.

5.16. Arrest of Stecco

Country: **Italy (p. 39)**
Date: **2017 - 2023**
Techniques used:
Covert surveillance devices > Audio (#1)
Covert surveillance devices > Location (#1)
Covert surveillance devices > Video (#1)
Mass surveillance > Civilian snitches (#1)
Mass surveillance > Video surveillance (#1)
Physical surveillance > Covert (#1)
Service provider collaboration > Mobile network operators (#1)
Service provider collaboration > Other (#1)
Targeted digital surveillance > Authentication bypass (#1)
Targeted digital surveillance > Malware (#1)

In the months preceding October 2023, Italian police tried to find and arrest Stecco, who was on the run.[102] Stecco was accused of helping another person on the run in 2017 and 2018 and of creating fake documents,[103] and also had a cumulative prison sentence of 3 years and 6 months to serve in relation to other cases.[104]

ankverfahren-gegen-drei-anarchistinnen-aus-hamburg-ist-jetzt-abgeschlossen

[98] https://soutienauxinculpeesdu8decembre.noblogs.org/post/2023/09/11/chronologie-de-laffaire

[99] https://web.archive.org/web/20240916210017/https://soutien812.blackblogs.org/2022/01/30/un-recit-de-laffaire-du-8-12

[100] https://web.archive.org/web/20241215183331/https://soutien812.blackblogs.org/2024/12/15/affaire-du-8-12-analyse-dune-enquete-preliminaire-pnat-et-dgsi

[101] https://soutienauxinculpeesdu8decembre.noblogs.org/post/2024/01/23/affaire-du-8-12-le-devenir-terroriste-des-luttes

[102] https://ilrovescio.info/2023/10/21/arrestato-stecco-in-aggiornamento

[103] https://actforfree.noblogs.org/2022/03/03/trentino-italy-repressive-operation-and-new-measures-against-anarchists

[104] https://notrace.how/resources/#cose-utili-da-sapere

Covert surveillance devices > Location (#1)
Covert surveillance devices > Video (#1)
Detection dogs (#1)
Forensics > DNA (#1)
Forensics > Linguistics (#1)
International cooperation (#1)
Mass surveillance > Video surveillance (#1)
Network mapping (#1)
Open-source intelligence (#1)
Physical surveillance > Aerial (#1)
Physical surveillance > Covert (#1)
Police patrols (#1)
Service provider collaboration > Mobile network operators (#1)
Service provider collaboration > Other (#1)
Targeted digital surveillance > Authentication bypass (#1)
Targeted digital surveillance > IMSI-catcher (#1)

In April 2022,[88] October 2022,[89] and February 2025[90] several raids took place as part of an investigation into the editors of the German anarchist newspaper Zündlumpen, published from 2019 to 2021. In February 2025 two people, N. and M., were arrested: they were accused of being editors of Zündlumpen and suspected of having committed several arsons.[91]

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

[88] https://actforfree.noblogs.org/2022/05/13/munich-germany-about-raids-and-a-%c2%a7129-procedure-against-anarchists-and-the-theft-of-a-printing-space

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

[90] https://actforfree.noblogs.org/2025/03/26/about-the-repressive-operation-in-germany-and-austria-solidarity-with-the-arrested-anarchists

[91] https://actforfree.noblogs.org/2025/07/03/munich-germany-update-on-the-imprisonment-of-the-two-comrades

5.13. Repression of the 2019 uprising in Chile

Country: **Chile (p. 39)**
Date: **2019 - 2020**
Techniques used:
Physical surveillance > Aerial (#1)
Physical violence (#1)

A series of protests and riots began in Chile in October 2019, following the announcement of an increase in the metro fare in Chile's capital, Santiago.[92] For several months, a large amount of public infrastructure and commercial buildings were vandalized, looted or burned in Santiago and elsewhere in the country.

In response to the unrest, the government deployed soldiers and imposed a curfew in a number of cities.[93] Many people were arrested and sentenced to years in prison.

5.14. The three from the park bench

Country: **Germany (p. 39)**
Date: **2019 - ?**
Techniques used:
Mass surveillance > Video surveillance (#1)
Physical surveillance > Covert (#1)

In 2019, three people were arrested while sitting on a park bench late at night in Hamburg,[94] accused of carrying incendiary devices[95] and planning to burn down a specific building whose address was written on a piece of paper found on them. Two of them had been followed by cops for several hours before their arrest.

In a 2020 trial, the people were sentenced to between 19 and 22 months in prison.[96] The sentences were upheld on appeal in 2022.[97]

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

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

[94] https://notrace.how/resources/#parkbank

[95] https://web.archive.org/web/20250612011456/https://parkbanksolidarity.blackblogs.org/509

[96] https://web.archive.org/web/20250612011456/https://parkbanksolidarity.blackblogs.org/end-of-the-trial-two-imprisoned-comrades-on-the-streets-again

[97] https://zuendlappen.noblogs.org/post/2022/06/06/hamburg-einmal-schneller-sein-als-die-presse-die-revision-im-sog-parkb

unlikely to be stumbled upon. A safe house is a house, apartment, or other space that an adversary doesn't know you're using.

Stash spots and safe houses each have advantages and disadvantages:

- It is easier to set up a stash spot.
- It is easier to **minimize DNA traces (p. 15)** in a stash spot.
- It is easier to change the location of a stash spot.
- A safe house provides more storage space and can be used for purposes other than storage such as sleeping, preparing materials, etc.

Examples of stash spots include:

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

Examples of safe houses include:

- A house, apartment, or other space rented with a **fake ID (p. 16)** and cash.
- The home of someone you trust and who is willing to take the risk this complicity entails, but who is far enough away from networks that are under surveillance.

If an adversary finds out about a stash spot or safe house, they can start monitoring it in order to identify you when you access it, as has happened in Italy where motion-activated cameras were installed to monitor a forest stash spot.[59] Because of this, when accessing a stash spot or safe house, you can:

- Practice **anti-surveillance (p. 7)** to counter the risk of physical surveillance.
- **Dress anonymously (p. 5)** to counter the risk of being observed or recorded.
- Practice **tamper-evident preparation (p. 23)** to ensure that the stash spot or safe house hasn't been accessed by an adversary.

[59] 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

[60] https://notrace.how/resources/#safe-houses

See "Security Culture and Safe Houses: Sustaining the Network, Nurturing Continuity"[60] for a historical perspective on the use of safe houses by anarchists.

4.30. Surveillance detection

Techniques addressed by this mitigation:
Covert surveillance devices > Video (#1)
Physical surveillance > Aerial (#1)
Physical surveillance > Covert (#1)

Surveillance detection is the practice of detecting if you are under **physical surveillance (#1)**, that is, detecting if you are being directly observed by an adversary. There are two types of surveillance detection: passive surveillance detection and active surveillance detection. Counter-surveillance is a sophisticated form of active surveillance detection.

Passive surveillance detection

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

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

Active surveillance detection

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

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

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

Counter-surveillance

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

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

Additional considerations

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

See also

- Surveillance Countermeasures[4] about the principles and techniques of surveillance detection.
- The "Physical surveillance" topic.[5]
- The related mitigation **Anti-surveillance (p. 7)**.

4.31. Tamper-evident preparation

Techniques addressed by this mitigation:

Targeted digital surveillance > Authentication bypass (#1)
Targeted digital surveillance > Physical access (#1)

A mixture of red and black lentils with a complex pattern. Electronic devices can be immersed in the mixture so that when they are accessed, the pattern changes.

Tamper-evident preparation is the process of taking precautionary measures to make it possible to detect

Service provider collaboration > Mobile network operators (#1)
Service provider collaboration > Other (#1)
Targeted digital surveillance > IMSI-catcher (#1)

In 2020, Boris was accused of sabotaging a cell tower in Besançon, Doubs, France, in March 2020, and two cell towers on Mount Poupet in the Jura Mountains, France, in April 2020.[83] He was initially suspected when his DNA was found on a bottle cap at the foot of one of the burnt cell towers on Mount Poupet. The charges against him for the sabotage of the Besançon cell tower were later dropped for lack of evidence.

In a trial in 2021, Boris was sentenced for the sabotage on Mount Poupet to two years in prison and a two-year suspended sentence. After his trial, he publicly claimed responsibility for the sabotage in a text entitled "Why I burned the two antennas on Mount Poupet".[84]

5.10. Search for a fugitive

Country: **United States (p. 40)**
Date: **2020 - ?**
Techniques used:

Door knocks (#1)
Forensics > DNA (#1)
Open-source intelligence (#1)
Physical surveillance > Covert (#1)
Service provider collaboration > Mobile network operators (#1)
Service provider collaboration > Other (#1)

In 2021 and 2022, as part of a state-level investigation in the state of Georgia, investigators attempted to locate and arrest a person suspected of being involved in a struggle against the construction of a police training center, and of drug trafficking.[85] In 2025, as part of a federal-level investigation, investigators again attempted to locate and arrest the person for allegedly participating in a 2020 attack against a United States Immigration and Customs Enforcement (ICE) building.

The person was not arrested and is in clandestinity.

[83] https://rupture.noblogs.org/post/2023/10/04/no-bars
[84] https://anarchistnews.org/content/why-i-burned-2-antennas
[85] Private source.

5.11. 2019-2020 case against Mónica and Francisco

Country: **Chile (p. 39)**
Date: **2019 - 2023**
Techniques used:

Forensics > DNA (#1)
Forensics > Facial recognition (#1)
Forensics > Handwriting analysis (#1)
Mass surveillance > Civilian snitches (#1)
Mass surveillance > Video surveillance (#1)
Open-source intelligence (#1)

A comparison diagram presented as evidence by the prosecutor. On the left, an alleged picture of Mónica, disguised, before an action. On the right, a picture of Mónica. Skin features such as moles are visible in the same place in both pictures.

In 2020, Mónica Caballero and Francisco Solar were arrested in Chile, accused of sending two parcel bombs—to a police station and a former Minister of the Interior—in 2019, and placing explosive devices in a park in an attempt to harm cops in 2020.[86] Both were charged with attempted murder.

In a trial in 2023, Francisco Solar was sentenced to 86 years in prison and Mónica Caballero to 12 years.[87]

5.12. Repression against Zündlumpen

Country: **Germany (p. 39)**
Date: **2019 - ?**
Techniques used:

Covert house visit (#1)
Covert surveillance devices > Audio (#1)

[86] https://notrace.how/resources/#monica-francisco
[87] https://informativoanarquista.noblogs.org/post/2023/12/08/chile-condenas-contra-lxs-companerxs-monica-caballero-y-francisco-solar

Cursive graffiti left at the action site, which helped identify the person.

In March 2023, a person was arrested[75] and charged with a May 2022 arson attack on the headquarters of an anti-abortion group.[76] The arson was the first in a series of attacks claimed under the name "Jane's Revenge"—a reference to the "Jane Collective", an underground organization that facilitated access to abortion in the United States from 1969 to 1973.

In a 2024 trial, the person was sentenced to 7 and a half years in prison.[77]

5.7. Repression of the attack on Clarín's headquarters

Country: **Argentina (p. 39)**
Date: **2021 - 2022**
Techniques used:

Forensics > Facial recognition (#1)
Forensics > Fingerprints (#1)
Forensics > Gait recognition (#1)
House raid (#1)
Mass surveillance > Video surveillance (#1)
Network mapping (#1)
Open-source intelligence (#1)
Service provider collaboration > Mobile network operators (#1)
Service provider collaboration > Other (#1)

In 2021 and 2022, several people were arrested and accused of throwing Molotov cocktails at the headquarters of Clarín, Argentina's largest newspaper, in 2021.[78]

In a 2022 trial, three of the defendants were sentenced to a three-year suspended prison sentence.[79]

5.8. Belarusian anarcho-partisans

Country: **Belarus (p. 39)**
Date: **2020 - 2021**
Techniques used:

Mass surveillance > Civilian snitches (#1)
Physical violence (#1)

In 2020, four people set fire to police buildings and to vehicles in the parking lot of a prosecutor's office.[80] Soon after, they were arrested by border guards while trying to cross the Belarusian-Ukrainian border.

In the first days of their detention, the people were tortured.[81] Eventually, all four took responsibility for carrying out the actions of which they were accused.

After a trial in 2021, they were sentenced to 18 to 20 years in prison.[82]

5.9. Case against Boris

Country: **France (p. 39)**
Date: **2020 - 2021**
Techniques used:

Covert surveillance devices > Location (#1)
Covert surveillance devices > Video (#1)
Forensics > DNA (#1)
ID checks (#1)
Interrogation techniques (#1)
Mass surveillance > Police files (#1)
Mass surveillance > Video surveillance (#1)
Physical surveillance > Covert (#1)

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

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

[77] https://madison.com/news/local/crime-courts/hridindu-roychowdhury-crime-abortion-madison-wisconsin/article_af329b98-f752-11ee-a846-632571f96ea2.html

[78] https://publicacionrefractario.wordpress.com/2022/03/23/argentina-detenidxs-companerxs-acusadxs-de-participar-en-el-atentado-incendiario-contra-el-periodico-el-clarin

[79] https://lanacion.com.ar/politica/condenan-a-tres-anos-de-prision-en-suspenso-a-tres-de-los-atacantes-del-diario-clarin-con-molotovs-nid07092022

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

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

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

when something has been **physically accessed (#1)** by an adversary.

Tamper-evident preparation can be used:

- To detect if an adversary has accessed an electronic device during a **covert house visit (#1)** (in which case they may have installed **malware (#1)** on the device).
- To detect if an adversary has accessed a **stash spot or safe house (p. 21)**.

Examples of tamper-evident preparation techniques include:

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

See AnarSec's guide "Make Your Electronics Tamper-Evident"[61] on how to use tamper-evident preparation for electronic devices.

[61] https://anarsec.guide/posts/tamper

4.32. Transportation by bike

Techniques addressed by this mitigation:

Covert surveillance devices > Location (#1)
Mass surveillance > Video surveillance (#1)
Physical surveillance > Covert (#1)

Transportation by bike is the practice of using a bicycle instead of other modes of transportation.

Advantages of transportation by bike include:

- Bikes are harder to identify through **video surveillance (#1)** than cars: the make and model of a bike can be obscured and bikes usually have no license plates.
- It is harder for a **physical surveillance (#1)** operation to follow a bike than a car or someone on foot, especially without being detected, and it is easier to conduct **surveillance detection (p. 22)** and **anti-surveillance (p. 7)** from a bike. For example, in a six-month physical surveillance operation against an anarchist in France, the police regularly lost track of him while he was biking.[62]
- There are far fewer places to install a **tracking device (#1)** on a bike than on a car, and when you **search (p. 10)** a bike, you can tell with a high degree of confidence whether a tracking device is present or not.

[62] https://notrace.how/resources/#ivan

5. Repressive operations

5.1. Case against Louna

Country: **France (p. 39)**
Date: **2024 - ?**
Techniques used:

- **Covert surveillance devices > Audio (#1)**
- **Covert surveillance devices > Location (#1)**
- **Covert surveillance devices > Video (#1)**
- **Forensics > Arson (#1)**
- **Forensics > DNA (#1)**
- **Guards (#1)**
- **House raid (#1)**
- **Mass surveillance > Civilian snitches (#1)**
- **Mass surveillance > Video surveillance (#1)**
- **Physical surveillance > Covert (#1)**
- **Service provider collaboration > Mobile network operators (#1)**
- **Service provider collaboration > Other (#1)**

On the night of May 4 to May 5, 2024, an excavator was set on fire at the construction site of a highway project.[63] On October 12, 2024, Louna was arrested and accused of setting the excavator on fire. Several other people were arrested and released soon after.

CCTV footage from the arson site showed two people setting fire to the excavator, and one of them burning themselves accidentally. In the hours following the arson, Louna was brought by car to a nearby hospital, where she was admitted for burns allegedly compatible with those visibly suffered by the person who burned themselves in the footage.

After her arrest, Louna was detained in isolation for four months—she was in isolation because she was in a men's prison despite being a (trans) woman.[64] After her arrest, she claimed responsibility for the degradations against the excavator. She is currently under judicial supervision pending trial.

[63] https://soutienlouna.noblogs.org/post/2025/01/23/free-louna-des-nouvelles-de-laffaire-de-louna-meuf-trans-anar-incarceree-dans-le-cadre-de-la-lutte-contre-la69

[64] https://soutienlouna.noblogs.org/post/2025/02/17/louna-est-sortie-de-prison-mais-nest-toujours-pas-libre

5.2. Berlin 2023 railway conspiracy case

Country: **Germany (p. 39)**
Date: **2023 - 2024**
Technique used:

- **Physical surveillance > Aerial (#1)**

In February 2023, a few minutes after midnight, during a routine surveillance flight, the helicopter of the German federal police identified two people on railroad tracks near Berlin.[65] Three police cars were dispatched to the location and the people were arrested on suspicion of attempted arson against the railway infrastructure.

In a 2024 trial, the two people were acquitted.[66]

5.3. Case against Peppy and Krystal

Country: **United States (p. 40)**
Date: **2023 - ?**
Techniques used:

- **Covert house visit (#1)**
- **Mass surveillance > Video surveillance (#1)**
- **Physical surveillance > Covert (#1)**
- **Service provider collaboration > Other (#1)**

In 2023, the home of Peppy and Krystal was raided, and both were arrested a month later.[67] Peppy was accused of launching two smoke bombs and a firework during a protest against a transphobic event, and Krystal was accused of conspiring with Peppy.[68]

After a 2024 trial, Peppy was sentenced to 5 years in prison and 3 years of supervised release, and Krystal was sentenced to 3 years of supervised release.

[65] https://notrace.how/resources/#conspiring

[66] https://de.indymedia.org/node/379250

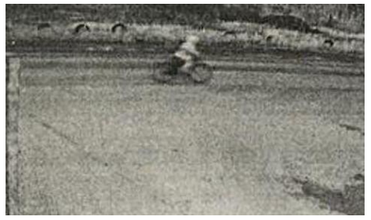
[67] https://freepeppyandkrystal.noblogs.org/timeline-and-detailed-updates

[68] https://notrace.how/documentation/case-against-peppy-and-krystal-affidavit.pdf

5.4. Case against Ruslan Siddiqi

Country: **Russia (p. 40)**
Date: **2023 - 2025**
Techniques used:

- **Forensics > DNA (#1)**
- **Forensics > Trace evidence (#1)**
- **Interrogation techniques (#1)**
- **Mass surveillance > Civilian snitches (#1)**
- **Mass surveillance > Video surveillance (#1)**
- **Physical violence (#1)**



Cropped CCTV picture from a factory near the train bombing site, showing someone —allegedly Ruslan Siddiqi—riding a bike shortly before the bombing.

In November 2023, Ruslan Siddiqi was arrested and accused of bombing a freight train three weeks earlier, on a track that was also used to transport military equipment in the context of the Russo-Ukrainian war.[69] The bombing derailed 19 wagons. He was also accused of attacking a military airfield a few months earlier using drones carrying explosives. The attack on the airfield did not cause any damage.[70]

After his arrest, Ruslan Siddiqi publicly claimed responsibility for the train bombing and the attack on the military airfield. He carried out both actions a few kilometers from his home and traveled to both sites by bike.

In a 2025 trial, Ruslan Siddiqi was sentenced to 29 years in prison.[71]

[69] https://anarchistnews.org/content/you-could-call-me-partisan-ruslan-siddiqi-recounts-his-anti-war-actions

[70] https://theins.ru/en/society/280988

[71] https://avtonom.org/en/news/anarchist-ruslan-siddiqui-sentenced-29-years-maximum-security-penal-colony

5.5. Repression of Lafarge factory sabotage

Country: **France (p. 39)**
Date: **2022 - ?**
Techniques used:

- **Forensics > DNA (#1)**
- **House raid (#1)**
- **Mass surveillance > Video surveillance (#1)**
- **Open-source intelligence (#1)**
- **Service provider collaboration > Other (#1)**
- **Targeted digital surveillance > Authentication bypass (#1)**
- **Targeted digital surveillance > Malware (#1)**

On June 5, 2023, about fifteen people were raided and arrested in France, accused of participating in the December 2022 sabotage of a factory of the French industrial company Lafarge.[72] The sabotage, which took place during the day and involved between 100 and 200 people,[73] caused around 6 million euros of damage.

On June 20, 2023, about eighteen more people were raided and arrested in France, some of them in connection with the Lafarge sabotage.[74]

5.6. Repression of the first Jane's Revenge arson

Country: **United States (p. 40)**
Date: **2022 - 2024**
Techniques used:

- **Forensics > Arson (#1)**
- **Forensics > DNA (#1)**
- **Forensics > Handwriting analysis (#1)**
- **Mass surveillance > Video surveillance (#1)**
- **Physical surveillance > Covert (#1)**

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

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

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