The Threat Library is a knowledge base of repressive techniques used by the enemies of anarchists and other rebels and repressive operations where they've been used —a breakdown and classification of actions that can be used against us. Its purpose is to help you think through what mitigations to take in a particular project and to navigate resources that go into more depth on these topics. In other words, it helps you arrive at appropriate operational security for your threat model.

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

Depending on your context, possession of certain documents may be criminalized or attract unwanted attention—be careful about what zines you print and where you store them.

Threat Library

Part 4/5

Mitigations

Threat Library
Part 1/5: Tutorial, Tactics
Part 2/5: Techniques A–I
Part 3/5: Techniques M–T
Part 4/5: Mitigations
Part 5/5: Repressive operations, Countries

Original publication by the No Trace Project

notrace.how/threat-library

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

July 11, 2024

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

See AnarSec's guide "Make Your Electronics Tamper-Evident"[60] on how to use tamper-evident preparation for electronic devices.

5.32. Transportation by bike

Techniques addressed by this mitigation:

Covert surveillance devices > Location (#2)
Mass surveillance > Video surveillance (#3)
Physical surveillance > Covert (#3)

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 (#3)** 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 (#3)** 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. 45)** 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[61].
- There are far fewer places to install a **tracking device (#2)** on a bike than on a car, and when you **search (p. 15)** a bike, you can tell with a high degree of confidence whether a tracking device is present or not.

[60] https://anarsec.guide/posts/tamper
[61] https://notrace.how/resources/#ivan

Tamper-evident preparation is the process of taking precautionary measures to make it possible to detect when something has been **physically accessed (#3)** by an adversary.

Tamper-evident preparation can be used:

- To detect if an adversary has accessed an electronic device during a **covert house visit (#2)** (in which case they may have installed **malware (#3)** on the device).
- To detect if an adversary has accessed a **stash spot or safe house (p. 44)**.

Examples of tamper-evident preparation techniques include:

- Applying nail polish to a laptop screws and taking pictures of the screws. Because nail polish has a complex pattern, it 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.
- 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.

Contents

5. Mitigations 3
5.1. Anonymous dress 3
5.2. Anonymous phones 5
5.3. Anonymous purchases 6
5.4. Anti-surveillance 7
5.5. Attack 10
5.6. Avoiding self-incrimination 11
5.7. Background checks 13
5.8. Biometric concealment 14
5.9. Bug search 15
5.10. Careful action planning 17
5.11. Clandestinity 17
5.12. Compartmentalization 18
5.13. Computer and mobile forensics 19
5.14. Digital best practices 20
5.15. DNA minimization protocols 28
5.16. Encryption 29
5.17. Fake ID 30
5.18. Gloves 31
5.19. Masking your writing style 33
5.20. Metadata erasure and resistance 34
5.21. Need-to-know principle 35
5.22. Network map exercise 37
5.23. Outdoor and device-free conversations 38
5.24. Physical intrusion detection 39
5.25. Preparing for house raids 40
5.26. Preparing for repression 41
5.27. Prisoner support 42
5.28. Reconnaissance 42
5.29. Stash spot or safe house 44
5.30. Surveillance detection 45
5.31. Tamper-evident preparation 48
5.32. Transportation by bike 50

5. Mitigations

5.1. Anonymous dress

Techniques addressed by this mitigation:

Forensics > Facial recognition (#2)
Forensics > Gait recognition (#2)
Forensics > Trace evidence (#2)
Mass surveillance > Civilian snitches (#3)
Mass surveillance > Video surveillance (#3)
Physical surveillance > Aerial (#3)
Physical surveillance > Overt (#3)

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. 14)**).

Ensure that clothing cannot be used to identify you

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[5] about the principles and tactics of surveillance detection.
- The physical surveillance topic[6].
- The related mitigation **Anti-surveillance (p. 7)**.

5.31. Tamper-evident preparation

Techniques addressed by this mitigation:

Targeted digital surveillance > Authentication bypass (#3)
Targeted digital surveillance > Physical access (#3)

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.

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

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

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 above.
2. Far away from the action site, change from your regular clothing into the civilian clothing, in a suitable place where there are no surveillance cameras or witnesses.
3. Close to the action site, change into the action clothing (in a suitable place).
4. Perform the action.
5. Close to the action site, change back into the civilian clothing (in a suitable place).
6. Far away from the action site, change back into your regular clothing (in a suitable place).
7. Dispose of the civilian clothing and the action clothing safely.

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.

5.2. Anonymous phones

Techniques addressed by this mitigation:

Network mapping (#3)

Service provider collaboration > Mobile network operators (#3)

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.

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 (#3)**.

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 (#3)**—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.

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.

- 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. 3)** to counter the risk of being observed or recorded.
- Practice **tamper-evident preparation (p. 48)** to ensure that the stash spot or safe house hasn't been accessed by an adversary.

5.30. Surveillance detection

Techniques addressed by this mitigation:

Covert surveillance devices > Video (#2)
Physical surveillance > Aerial (#3)
Physical surveillance > Covert (#3)

Surveillance detection is the practice of detecting if you are under **physical surveillance (#3)**, 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

[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

- Burner Phone Best Practices[2] for more information on burner phones.

5.3. Anonymous purchases

Techniques addressed by this mitigation:

Forensics > Arson (#2)
Forensics > Ballistics (#2)
Mass surveillance > Video surveillance (#3)
Service provider collaboration > Other (#3)

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 (#2)**) 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 (#3)**, 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.

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

- 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. 50)**), and do not bring a phone.
- Conduct **anti-surveillance (p. 7)** before going to the store.
- Use some level of **anonymous dress (p. 3)** 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[3].

See also

See Prisma[4] for more details on physical anonymous purchases.

5.4. Anti-surveillance

Techniques addressed by this mitigation:

Physical surveillance > Aerial (#3)
Physical surveillance > Covert (#3)

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

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

5.29. Stash spot or safe house

Techniques addressed by this mitigation:

Covert house visit (#2)
Covert surveillance devices > Video (#2)
Forensics > Ballistics (#2)
Forensics > Trace evidence (#2)
House raid (#2)

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 (#2)** or a **covert visit (#2)** of your residence. A stash spot is a hidden place, often outdoors, that is unlikely to be stumbled upon. A safe house is a house, apartment, or other space that an adversary doesn't know you're using.

Stash spots and safe houses each have advantages and disadvantages:

- It is easier to set up a stash spot.
- It is easier to **minimize DNA traces (p. 28)** 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. 30)** and cash.

Guards (#2)
Mass surveillance > Video surveillance (#3)
Police patrols (#3)

Reconnaissance is the gathering of information about the target of an action. It precedes **action planning (p. 17)**. 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 (#3)** coverage and a suitable place to change clothing before the action.
- Inspecting the action site itself, looking for surveillance cameras, **guards (#2)**, **alarm systems (#2)** 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. 3)** 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. 20)**.

Anti-surveillance is the practice of taking active measures to evade ("shake off") a **mobile physical surveillance operation (#3)**.

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

- 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.

5.27. Prisoner support

Techniques addressed by this mitigation:
Informants (#2)

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.

5.28. Reconnaissance

Techniques addressed by this mitigation:
Alarm systems (#2)

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

In addition, to detect if an adversary has **physically accessed (#3)** an electronic device during a covert house visit, you can use **tamper-evident preparation (p. 48)**.

5.26. Preparing for repression

Techniques addressed by this mitigation:

House raid (#2)
Physical violence (#3)

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

Examples of practical preparation include:

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

Examples of psychological preparation include:

can see far ahead and behind you to a small forest path, then accelerate, go deep into the forest, and come out of the forest far from where you entered, in a place that a surveillance 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[5] about the principles and techniques of anti-surveillance.
- The physical surveillance topic[6].
- The related mitigation **Surveillance detection (p. 45)**.

5.5. Attack

Techniques addressed by this mitigation:

Alarm systems (#2)
Guards (#2)
Increased police presence (#2)
Infiltrators (#2)
Informants (#2)
Mass surveillance > Civilian snitches (#3)
Mass surveillance > Police files (#3)
Mass surveillance > Video surveillance (#3)

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

Physical surveillance > Aerial (#3)
Police patrols (#3)

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[7] and P25[8] antennas, and police operations depend on the integrity of their vehicle fleets, stations, and individual officers' feelings of safety. The possibilities for attack are limited only by one's imagination.

5.6. Avoiding self-incrimination

Techniques addressed by this mitigation:

Door knocks (#2)
Forensics > Digital (#2)
ID checks (#2)
Interrogation techniques (#2)
Mass surveillance > Mass digital surveillance (#3)
Network mapping (#3)
Open-source intelligence (#3)

Avoiding self-incrimination means not giving information to an adversary that could be used to incriminate you or your

[7] https://en.wikipedia.org/wiki/Terrestrial_Trunked_Radio#Usage
[8] https://en.wikipedia.org/wiki/Project_25

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

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

5.25. Preparing for house raids

Techniques addressed by this mitigation:

Covert house visit (#2)
House raid (#2)

Preparing for house raids is the process of taking precautionary measures to minimize the impact of a potential **house raid (#2)** or **covert house visit (#2)**.

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. 29)**, 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. 44)**, 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.

Outdoor conversations can be recorded with covert microphones or long-range parabolic microphones during a **physical surveillance (#3)** 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. 34)** 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 being transmitted, which could happen when the phone later reconnects to the network.

See the security culture topic[55].

5.24. Physical intrusion detection

Techniques addressed by this mitigation:

Covert house visit (#2)
Covert surveillance devices > Audio (#2)
Covert surveillance devices > Location (#2)
Covert surveillance devices > Video (#2)
Evidence fabrication (#2)
Targeted digital surveillance > Physical access (#3)

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 (#2)**. 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.

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

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 a State adversary, 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 the police interrogate and how to defend against it[9] (in French and German) on how to defend against police interrogation techniques.

Need-to-know principle

Apply the **need-to-know principle (p. 35)**. 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. 20)**. 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.

[9] https://notrace.how/resources/#police-interroge

- Do not use social media, or at least do not post anything incriminating on social media. Social media is a treasure trove for State adversaries.
- Do not take photos or videos during riots. Taking photos or videos during riots incriminates people and should be considered a form of snitching[10].

5.7. Background checks

Techniques addressed by this mitigation:
Infiltrators (#2)
Informants (#2)

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:

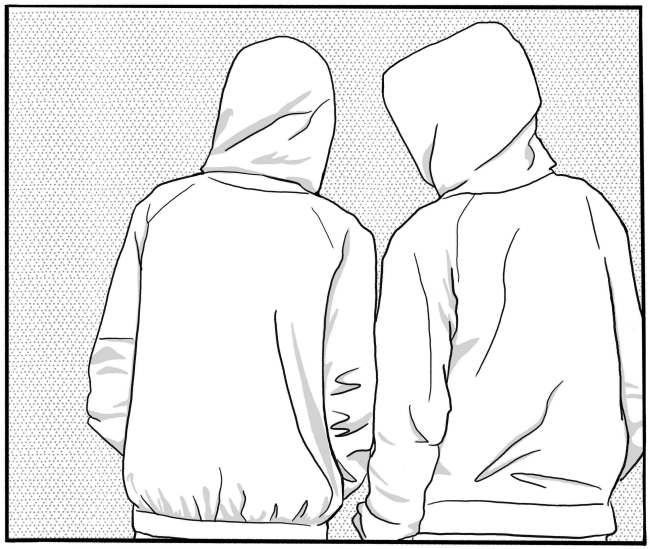
- The consensual, mutual approach: If you already trust someone to some degree but would like to trust them more, you can do a mutual background check, where each of you checks the other.
- The non-consensual approach: If you already have strong suspicions that someone is lying about their identity,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

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

struct during **network mapping (#3)**—so it should be burned immediately after use.

5.23. Outdoor and device-free conversations

Techniques addressed by this mitigation:
Covert surveillance devices > Audio (#2)
Mass surveillance > Video surveillance (#3)



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 (#2)**.
- Electronic devices can be infected with **malware (#3)** that can turn them into covert microphones.

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

5.22. Network map exercise

Techniques addressed by this mitigation:

Infiltrators (#2)
Informants (#2)
Network mapping (#3)
Targeted digital surveillance > Physical access (#3)

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 (#2)** 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 con-

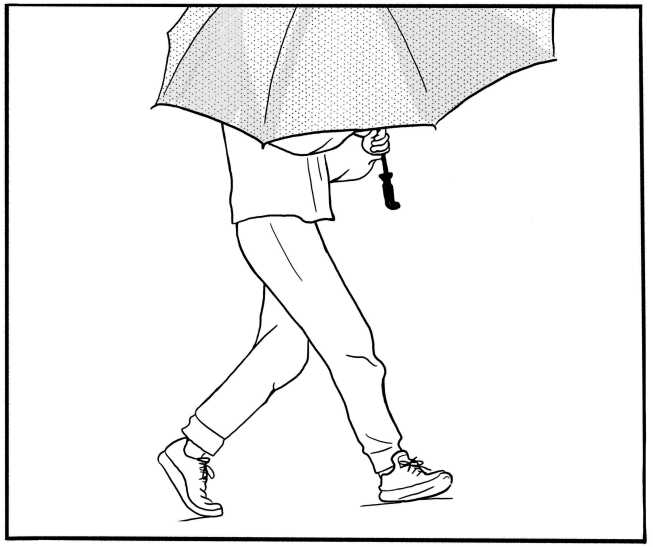
[54]https://notrace.how/resources/#secrets-lies
[55]https://notrace.how/resources/#topic=security-culture
[56]https://notrace.how/resources/#stop-hunting

For more information on background checks, see Confidence, Courage, Connection, Trust[11].

5.8. Biometric concealment

Techniques addressed by this mitigation:

Forensics > Facial recognition (#2)
Forensics > Gait recognition (#2)
Forensics > Handwriting analysis (#2)
Forensics > Linguistics (#2)
Mass surveillance > Video surveillance (#3)



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[4].

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

5.9. Bug search

Techniques addressed by this mitigation:

Covert surveillance devices > Audio (#2)
Covert surveillance devices > Location (#2)
Covert surveillance devices > Video (#2)
Targeted digital surveillance > Authentication bypass (#3)
Targeted digital surveillance > IMSI-catcher (#3)

A bug search is the active process of trying to detect the presence of **covert surveillance devices (#2)** 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. 38)**.

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.

Informants (#2)
Network mapping (#3)

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 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:

- 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. 20)** 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. 20)**.

See also

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

5.21. Need-to-know principle

Techniques addressed by this mitigation:

Biased interpretation of evidence (#2)
Infiltrators (#2)

[51] https://eff.org/issues/printers
[52] https://github.com/tpet/mat2
[53] https://anarsec.guide/posts/metadata

- 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. 50)**, 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. 45)**.

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.

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

5.10. Careful action planning

Techniques addressed by this mitigation:

Detection dogs (#2)
Forensics > Arson (#2)
Forensics > DNA (#2)
Forensics > Fingerprints (#2)
Forensics > Trace evidence (#2)
Increased police presence (#2)
Mass surveillance > Civilian snitches (#3)
Police patrols (#3)

When planning an action, careful action planning is the sensible development of the action plan. It follows **reconnaissance (p. 42)**.

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?

5.11. Clandestinity

Techniques addressed by this mitigation:

Covert house visit (#2)
House raid (#2)

Clandestinity is the process of breaking away from your established identity and begin a new life with a **fake identity (p. 30)**.

- 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 (#2)** or **covert house visit (#2)**, and generally avoid publishing texts in your name throughout your life.

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

5.20. Metadata erasure and resistance

Techniques addressed by this mitigation:

Forensics > Digital (#2)

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.

[49] https://anonymousplanet.org/guide.html#appendix-a4-counteracting-forensic-linguistics
[50] https://notrace.how/resources/#who-wrote

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. 3)**.

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).

5.19. Masking your writing style

Techniques addressed by this mitigation:
Forensics > Linguistics (#2)

Masking your writing style is the practice of altering the way you write to counter author identification by **forensic linguistics (#2)**.

For example:

[47] https://notrace.how/resources/#topic=fingerprints
[48] https://militanz.blackblogs.org/163-2

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].

5.12. Compartmentalization

Techniques addressed by this mitigation:
Network mapping (#3)
Targeted digital surveillance > Malware (#3)
Targeted digital surveillance > Network forensics (#3)

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 (#3)**, the compromise won't spread to other sticks or virtual machines.

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

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. 35)** 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.

5.13. Computer and mobile forensics

Techniques addressed by this mitigation:
Targeted digital surveillance > Malware (#3)
Targeted digital surveillance > Physical access (#3)

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

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 organization AccessNow[17], with the caveat that they are a legal organization that might be forced to share with the State data that you provide them.

[15]https://tails.net
[16]https://www.qubes-os.org
[17]https://accessnow.org/help

- 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. 28)**.

Hand characteristics

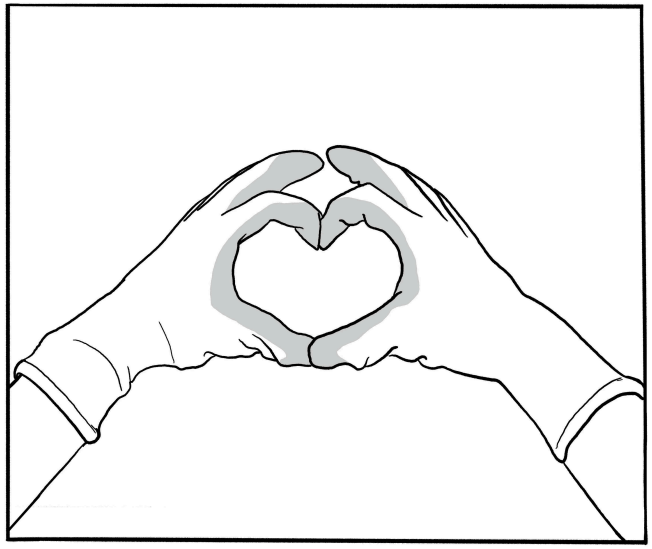
[45]https://en.wikipedia.org/wiki/Glove_prints
[46]To do this, pinch the inside of the left glove with your right hand and put your left hand into it (if you're right-handed, otherwise reverse), then pinch the outside of the right glove with your left gloved hand and put your right hand into it.

- To establish a **safe house (p. 44)**.
- To take the path of **clandestinity (p. 17)**.

5.18. Gloves

Techniques addressed by this mitigation:

Forensics > DNA (#2)
Forensics > Fingerprints (#2)



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.

See also:

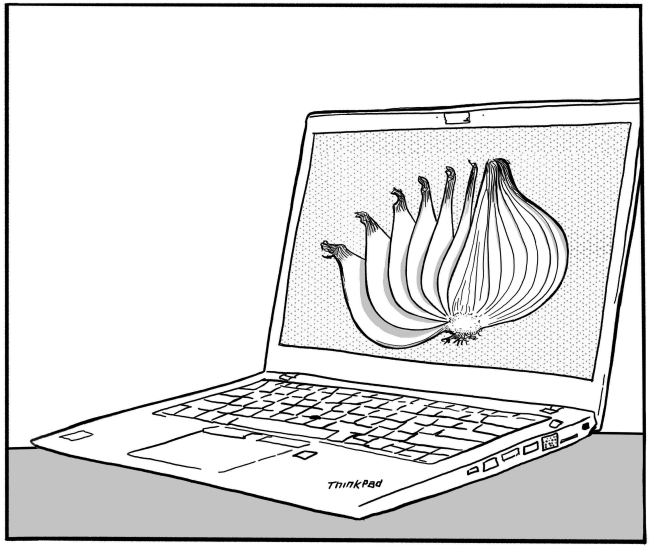
- The Device Integrity[18] page on Privacy Guides.
- Practical Linux Forensics[19] for a comprehensive introduction to the skill set on Linux, the platform most relevant to anarchists and other rebels.

5.14. Digital best practices

Techniques addressed by this mitigation:

Alarm systems (#2)
Biased interpretation of evidence (#2)
Covert surveillance devices > Video (#2)
Door knocks (#2)
Doxing (#2)
Forensics > Digital (#2)
Mass surveillance > Mass digital surveillance (#3)
Network mapping (#3)
Service provider collaboration > Mobile network operators (#3)
Service provider collaboration > Other (#3)
Targeted digital surveillance > Authentication bypass (#3)
Targeted digital surveillance > Malware (#3)
Targeted digital surveillance > Network forensics (#3)
Targeted digital surveillance > Physical access (#3)

[18] https://privacyguides.org/en/device-integrity
[19] 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, there are a number of best practices that you can follow when using digital devices.

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 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.

(#2), or **covert house visit (#2)** while it is turned off, the adversary will not be able to access its data (unless they **bypass its authentication (#3)**).

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. 20)** 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. 38)**.

5.17. Fake ID

Techniques addressed by this mitigation:
ID checks (#2)
Network mapping (#3)

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 (#3)** or avoid arrest in the event of an **ID check (#2)**.

- 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].

5.16. Encryption

Techniques addressed by this mitigation:

Forensics > Digital (#2)
Mass surveillance > Mass digital surveillance (#3)
Service provider collaboration > Mobile network operators (#3)
Service provider collaboration > Other (#3)
Targeted digital surveillance > IMSI-catcher (#3)
Targeted digital surveillance > Malware (#3)
Targeted digital surveillance > Network forensics (#3)

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. 20)**. 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**

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

Use security-oriented operating systems

Use:

- Debian[20] or Qubes OS[21] for daily computer use. See AnarSec's guide "Qubes OS for Anarchists"[22] 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"[23] and "Tails Best Practices"[24].
- GrapheneOS[25] for phones. See AnarSec's guide "GrapheneOS for Anarchists"[26].

Do not use Windows, MacOS, iPhones, and stock Android.

Encrypt your devices

Enable **Full Disk Encryption (p. 29)** on all your digital devices.

Use strong passwords

Most of your passwords (e.g. passwords you use to log in to websites) should be generated by and stored in a password manager—we recommend KeePassXC[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).

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

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).

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

[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://www.eff.org/dice

5.15. DNA minimization protocols

Techniques addressed by this mitigation:

Forensics > DNA (#2)

DNA minimization protocols allow you to manipulate objects while minimizing the amount of **DNA (#2)** 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.

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. 29)** using a strong password, an adversary could **bypass the encryption (#3)**.
- 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 (#3)** 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 (#2)** 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

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 (#3)**).

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, 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.

[31] https://torproject.org

- 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 conduct any Internet activity 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].

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 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].

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

Back up your digital data

[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

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

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. 29)**. 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 (#2)** 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. 48)**.

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 (#2)**. 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 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