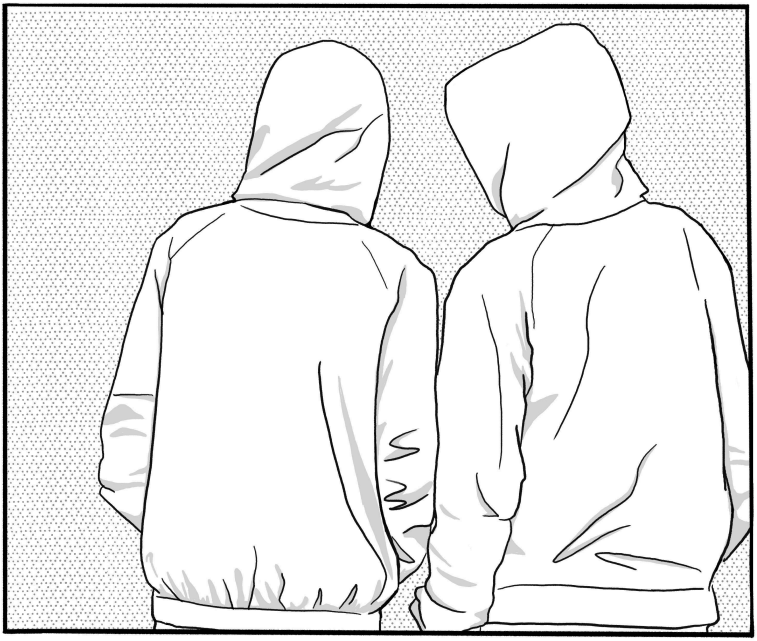
Threat Library



November 4, 2025

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

Threat Library

Original text in English

No Trace Project

notrace.how/threat-library

Contents

1. About the Threat Library

> No matter what, we make and will continue to make mistakes in the battle against such strong oppressive mechanisms. Mistakes that will always "cost" more compared to the cops' mistakes which are "absorbed." We must weigh the situations again and ensure that the mistakes which happened once simply can not happen again. We must study and appreciate the accumulated experience of so many years and, taking into account the tendency to prepare for the battles which already took place and not for those that will come, let's be prepared and may luck be on our side…
>
> *— anarchist comrades from Greece, in a text[1] detailing the surveillance that led to their arrest, 2013*

1.1. Threat modeling

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

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

1.2. The Threat Library

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

[1] https://notrace.how/resources/#nea-filadelphia

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

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

1.3. Limitations

The Threat Library is by design a very technical approach to anti-repression. Threat modeling is done at the level of actions, and thus does not attempt to contribute to the social question, how to escape the enclosure that repression seeks, how to intervene in social tensions, and so on. Struggles

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

[a] https://notrace.how/resources/#not-stupid

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

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

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

2. Tactics

2.1. Deterrence

Uses techniques:

Door knocks (p. 31)
Doxing (p. 32)
Increased police presence (p. 77)
Mass surveillance (p. 85)
Physical violence (p. 108)
Police patrols (p. 111)

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

2.2. Incrimination

Uses techniques:

Biased interpretation of evidence (p. 13)
Covert house visit (p. 15)
Covert surveillance devices (p. 16)
Detection dogs (p. 26)
Door knocks (p. 31)
Evidence fabrication (p. 32)
Forensics (p. 33)
House raid (p. 72)
ID checks (p. 76)
Infiltrators (p. 78)
Informants (p. 80)
International cooperation (p. 82)
Interrogation techniques (p. 83)

Mass surveillance (p. 85)
Network mapping (p. 95)
Open-source intelligence (p. 97)
Parallel construction (p. 98)
Physical surveillance (p. 99)
Physical violence (p. 108)
Police patrols (p. 111)
Roadblocks (p. 112)
Service provider collaboration (p. 113)
Targeted digital surveillance (p. 125)

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

2.3. Arrest

Uses techniques:

Alarm systems (p. 12)
Detection dogs (p. 26)
Guards (p. 71)
House raid (p. 72)
ID checks (p. 76)
Increased police presence (p. 77)
International cooperation (p. 82)
Police patrols (p. 111)
Roadblocks (p. 112)

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

3. Techniques

3.1. Alarm systems

Used in tactic: **Arrest**

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

For physical infrastructure, modern alarm systems typically include sensors that detect unauthorized access to an area outside of normal operating hours. Such sensors include infrared motion detectors, sensors that detect the opening of doors, and many other types of sensors.[3] The alert signal can be sent over a wired or wireless connection—low-cost modern systems often send the signal over the mobile phone network.

For digital infrastructure, intrusion detection systems[4] monitor for any activity that might indicate a hack is in progress. If unauthorized access is detected, an incident response team can be notified to attempt to contain and remediate any compromise.

Mitigations

Attack (p. 143): You can attack alarm systems or the communication lines they use to send alert signals. For example, you can destroy alarm systems or jam alert signals with a jamming device.

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

[3] https://en.wikipedia.org/wiki/Security_alarm#Sensor_types
[4] https://en.wikipedia.org/wiki/Intrusion_detection_system

Digital best practices (p. 152): When carrying out a cyber action, you can use digital evasion techniques[5] to prevent intrusion detection systems from detecting the action.

Reconnaissance (p. 173): Before an action, you can survey the target building or infrastructure to determine the presence of an alarm system, and the type and location of sensors or other alarm devices.

3.2. Biased interpretation of evidence

Used in tactic: **Incrimination**

Biased interpretation of evidence is the practice of interpreting evidence in favor of a particular point of view.

Biased interpretation of evidence is the standard practice of modern justice systems which tend to favor the rich and powerful and discriminate against anarchists and other rebels. Evidence is interpreted with bias at all levels: when it is collected by investigators, when it is presented by prosecutors, and when it is considered by judges. Any information (even mundane information) can be woven into a narrative to fit the purposes of an investigation.

Mitigations

Digital best practices (p. 152): You can follow digital best practices to limit the information an adversary has about you, and therefore limit the information they can interpret in a biased way.

Need-to-know principle (p. 167): You can apply the need-to-know principle to limit the information an adversary has about you, and therefore limit the information they can interpret in a biased way.

Repressive operations

Operation 8 (p. 209): The case was characterized by a lack of evidence that the defendants were planning a specific attack, and relied instead on interpretation of circumstantial evidence.[6] For example:

[5] https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques
[6] https://putatara.net/2013/11/25/operation-8-the-evidence

- Activities captured by hidden cameras at the "training camps"—training with firearms, learning military tactics, experimenting with Molotov cocktails—were intepreted as preparation for violently seizing control of part of New Zealand's territory.
- In private conversations recorded by microphones installed in vehicles, some defendants made boasting or unserious comments, including about "going to war," acquiring a long-range sniper rifle, assassinating George W. Bush, or killing Pākehā (New Zealanders of European descent). These comments were interpreted as indicative of violent intentions.[7]

December 8 case (p. 193): The case was characterized by a lack of evidence that the defendants were planning a specific attack, and relied instead on interpretation of circumstantial evidence.[8] For example:

- Libre Flot gained combat experience in Rojava, which was interpreted as an attempt to gain experience in order to carry out attacks in France.
- Libre Flot stole fertilizer from a store, intending to use it to create small explosives. The theft was interpreted as an attempt to obtain fertilizer without leaving traces.
- On two occasions, some of the defendants created small explosives from household or agricultural products, and detonated them in isolated areas where the explosions would not damage anything, which was interpreted as tests for possible future attacks (despite the defendants' claims that they were just doing it for fun).
- Some of the defendants participated in airsoft games, which were intepreted as paramilitary trainings.
- Handwritten notes of one of the defendants contained terms and phrases such as "weapons", "recruitment", "cleaning DNA", "incendiary device" and "are we ready for a comrade to be wounded or killed?", which were interpreted as indicative that the defendant was preparing an attack in France (despite the defendant's claims that the notes were about either airsoft or Rojava).

[7]Private source.

[8]https://web.archive.org/web/20250615210912/https://soutien812.blackblogs.org/wp-content/uploads/sites/1922/2023/11/CompteRenduProces_A4.pdf

- In private conversations, some of the defendants made light-hearted, boasting comments such as "I want to burn all the banks, all the cops" and "if a police officer was on ground, honestly I would finish him off", which were interpreted as indicative of violent intentions.
- The defendants used secure digital communication tools, which was interpreted as indicative of "clandestine behavior".

3.3. Covert house visit

Used in tactic: **Incrimination**

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

An adversary can conduct a covert house visit to:

- Gather information.
- Install **covert surveillance devices (p. 16)** in the residence.
- Install **malware (p. 131)** on digital devices.

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

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

In addition to visiting the residence, the adversary can covertly seize garbage from outside the residence in the hope of finding valuable information (e.g., written notes, forensics evidence such as DNA traces).

Mitigations

Clandestinity (p. 150): If you enter clandestinity, an adversary cannot know where you live, and therefore cannot conduct a covert house visit of your home.

Physical intrusion detection (p. 170): You can use physical intrusion detection to detect a covert house visit.

Preparing for house raids (p. 171): You can prepare for a covert house visit by minimizing the presence of materials that could be harmful in the event of a visit.

Stash spot or safe house (p. 174): You can keep action materials that have no "legitimate" purpose in a stash spot or safe house, or at worst, let them pass through your home only for a very limited time.

Repressive operations

Repression against Zündlumpen (p. 191): Investigators made a covert visit of the cabins where N. and M. lived in order to collect **scent samples (p. 26)**.[9]

Case against Peppy and Krystal (p. 183): Investigators conducted a covert search of the trash outside the home of Peppy and Krystal, where they found suspicious documents.[10]

Case against Direct Action (p. 212): After overhearing (presumably during a **physical surveillance (p. 99)** operation) that four members of Direct Action who lived together in a house were leaving the house for two days to go camping, investigators conducted two covert visits of the house over those two days:[11]

- On the first day, they visited the house to find a good place to install hidden microphones the next day and to check for possible booby traps.
- On the second day, they visited the house to install hidden microphones and take photographs of suspicious items and documents.

3.4. Covert surveillance devices

Used in tactic: **Incrimination**

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

[9] https://de.indymedia.org/node/548259

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

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

Where

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

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

When

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

- Most often, when it is retrieved by its installers.
- In some cases, when it is inadvertently discovered and removed by a third party.
- In rare cases, when it is deliberately discovered (through a **bug search (p. 147)**) and removed by a third party.

Power supply

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

Data transmission

Covert surveillance devices often transmit the data they collect:

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

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

See also

- Ears and Eyes.[12]
- The "Hidden devices" topic.[13]

3.4.1. Audio

A microphone found inside a neon ceiling light in Modena, Italy, in December 2015.[14]

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

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

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

[12] https://notrace.how/earsandeyes
[13] https://notrace.how/resources/#topic=hidden-devices
[14] https://notrace.how/earsandeyes/#modena-2015-12

Covert audio surveillance devices can be very sensitive and successfully pick up conversations even when there is loud music playing in the background or people are whispering. They can be extremely small—just a few millimeters—especially if they record locally (e.g. on an SD card) and do not transmit their recordings.

Recorded conversations can be used as evidence in court if incriminating matters are discussed, or if they can be misconstrued to appear incriminating in the eyes of a judge. Non-incriminating, mundane conversations can reveal a great deal about the targets of surveillance and help in **network mapping (p. 95)**.

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

Mitigations

Bug search (p. 147): You can conduct a bug search to locate covert audio surveillance devices and eventually remove them.

Outdoor and device-free conversations (p. 169): You can conduct sensitive conversations outdoors and without electronic devices to prevent an adversary from recording those conversations with covert audio surveillance devices.

Physical intrusion detection (p. 170): An adversary often needs to covertly enter a space to install a covert audio surveillance device in the space. You can use physical intrusion detection to detect such a covert entry.

Repressive operations

Repression against Zündlumpen (p. 191): Microphones were installed:[9]

- In a forest, in or around the cabins where N. and M. lived.
- In N.'s car, after N. left it unattended for a few hours.

Renata (p. 200): Six hidden microphones and a camera were found in a house after the operation.[15] The microphones were found in the living room, hallway, and bedrooms. The camera was found in the intercom system.

[15] https://web.archive.org/web/20201031014052/https://roundrobin.info/2019/03/trento-sei-microspie-e-una-telecamera-immagini-pesanti

See the corresponding Ears and Eyes case.[16]

Arrest of Stecco (p. 194): Microphones were installed in two homes, one collective space, and several cars.[17]

Case against Louna (p. 182): A hidden microphone was installed in a vehicle.[7]

Scintilla (p. 201): Microphones hidden in a house for two and a half years recorded conversations that the investigators used to prove that the defendants knew each other, talked regularly, worried about the creation of a DNA database and the impossibility of resisting DNA collection, and discussed writing a text to be published.[18]

See the corresponding Ears and Eyes case.[19]

Operation 8 (p. 209): Microphones were installed in several vehicles and homes.[6]

Case against Direct Action (p. 212): Investigators installed hidden microphones:[11]

- In the house where four members of Direct Action lived.
- In the apartment where the fifth member of Direct Action lived.

One day, after overhearing (presumably during a **physical surveillance (p. 99)** operation) that a member of Direct Action and his girlfriend were planning to have lunch at a cafe later in the day, investigators, with the cooperation of the cafe owner, quickly took the following steps:

- They installed a hidden microphone in a rubber plant inside the cafe.
- They replaced a waiter with a surveillance operator who made sure that the member of Direct Action and his girlfriend sat at a table near the plant.

December 8 case (p. 193): A hidden microphone was installed in the truck where Libre Flot lived.[20] When the legal authorization for installing

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

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

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

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

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

and using the microphone expired after two months, the microphone was remotely deactivated but not removed from the truck. It was removed several months later during the raids.

Another hidden microphone was installed in a small cabin used by some of the defendants.

3.4.2. Location

A GPS tracker found under a vehicle in Berlin, Germany, in August 2022.[21]

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

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

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

- Most often using GPS.
- In some cases, using alternatives to GPS such as GLONASS or satellite phone services.

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

- In rare cases, by emitting radio waves that are received by a nearby surveillance operator (typically in a vehicle following the target's vehicle).

Collected location data can be used as evidence in court. Non-incriminating, mundane location data can reveal a lot about the targets of surveillance and help in **network mapping (p. 95)**.

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

Mitigations

Bug search (p. 147): You can conduct a bug search to locate covert location surveillance devices and eventually remove them.

Physical intrusion detection (p. 170): An adversary often needs to covertly enter the space where a vehicle is parked to install a covert location surveillance device on the vehicle. You can use physical intrusion detection to detect such a covert entry.

Transportation by bike (p. 180): You can use a bike instead of any other type of vehicle: unlike other vehicles, when you conduct a **bug search (p. 147)** of a bike you can determine with a high degree of confidence whether or not a covert location surveillance device is installed on the bike.

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

Repressive operations

Case against Boris (p. 188): GPS tracking devices were placed under several vehicles after investigators learned that Boris—who did not have a driver license—was being transported in them.[22]

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

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

Repression against Zündlumpen (p. 191): A GPS tracker was installed on N.'s car.[9]

Arrest of Stecco (p. 194): GPS trackers were installed on 12 cars.[17]

A tracking device was installed on a bike that was suspected of being used by Stecco.

Case against Louna (p. 182): Several GPS trackers were installed on vehicles.[7]

Bure criminal association case (p. 196): Investigators installed a covert location tracker on a vehicle, where it remained for about a month.[7]

December 8 case (p. 193): A covert location tracker was installed on a vehicle used by Libre Flot.[20]

3.4.3. Video

A camera found in the skylight of a public school in Berlin, Germany, in July 2011.[23]

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

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

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

- The living room of a target.
- The windows of a building close to the home of a target, with a line of sight on the entrance of the home.
- Close to **stash spots or safe houses (p. 174)** as has happened in Italy, where motion-activated cameras were installed to monitor a forest stash spot.[24]

Captured images can be used as evidence in court. Non-incriminating, mundane images can reveal a lot about the targets of surveillance and help in **network mapping (p. 95)**.

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

Mitigations

Bug search (p. 147): You can conduct a bug search to locate covert video surveillance devices and eventually remove them.

Digital best practices (p. 152): An adversary can install covert video surveillance devices that can film a computer or phone screen, or a computer keyboard. To mitigate this, when using a computer or phone for sensitive activities, you can:

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

Physical intrusion detection (p. 170): An adversary often needs to covertly enter a space to install a covert video surveillance device in the space. You can use physical intrusion detection to detect such a covert entry.

Stash spot or safe house (p. 174): You can keep action materials in a stash spot or safe house to avoid bringing them into your home, where covert video surveillance devices can be present.

[24]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

Surveillance detection (p. 176): An adversary can park a surveillance vehicle near your home with a camera that films your home entrance. To mitigate this, you can use the following passive surveillance detection technique. It only works if you live in a place where there aren't too many different vehicles that park, that is, in some residential areas in cities and in most rural areas. Each time you leave or enter your home, you take note of all the vehicles parked on the street that have a line of sight to your home. Trying not to look suspicious, you note their model, color, and license plate number, either remembering the information or writing it down. After doing this for a while, you will become familiar with the "baseline" of vehicles that park on your street, which will be the vehicles of people who live nearby or their guests. Once you're familiar with the baseline, you'll be able to spot vehicles that are not part of that baseline and discreetly examine them to see if they are surveillance vehicles.

Repressive operations

Case against Boris (p. 188): Cameras were installed in the streets outside Boris's home and outside the home of someone close to him to film the entrances to the homes.[22]

Repression against Zündlumpen (p. 191): Cameras were installed:[9]

- In a forest, around the cabins where N. and M. lived.
- In a basement rented by N.
- In the apartments of people suspected of being close to N. and M.
- On a railway bridge with a path for pedestrians and bicycles. Investigators claimed to have recognized M. in the camera footage crossing the bridge on a bicycle around the time an arson occurred a few kilometers from the bridge.

Arrest of Stecco (p. 194): Cameras were installed:[17]

- In front of six homes.
- In cars.
- Inside train stations, providing investigators with real-time access to footage of the stations, which the cameras already installed in the stations did not provide.

Case against Louna (p. 182): Cameras were installed to film the entrances of several places where people opposed to the highway project lived.[7]

Operation 8 (p. 209): Cameras were installed at the "training camps" on several occasions.[6] They were installed shortly before the beginning of the camps and removed shortly after. The goal was to identify who was participating in the camps, what they were doing, and what they were wearing. Footage captured by these cameras showed people:

- Training with firearms.
- Learning military tactics: patrolling, counter-ambush drills, etc.
- Experimenting with Molotov cocktails.

At least one camera was installed outside a person's home.

December 8 case (p. 193): A camera was installed outside a small cabin used by some of the defendants, filming the cabin.[20] It was seemingly installed about 10 meters from the cabin, on a tree trunk.

3.5. Detection dogs

Used in tactics: **Arrest**, **Incrimination**

A police dog tracking a suspect in an industrial area, in the United States in 2018.

Detection dogs are dogs trained and used by an adversary to detect odors. Detection dogs can be used to detect substances such as explosives or drugs, track people, and participate in scent lineups to determine if a person's scent is present on an item.

An odor is caused by volatile chemical compounds emitted by a substance. For example, the odor of an old book is caused by chemical compounds released into the air by its pages, which are constantly decomposing.

Human scent, the odor of a human body, is caused by chemical compounds emitted by water secretions (sweat), oil secretions (sebum), skin flakes, and body openings (mouth, nose, etc.) Each person has a relatively unique scent that is relatively stable over time.

The sense of smell of dogs is much more complex and developed than that of humans. Dogs can:

- Detect very faint odors.
- Detect a single odor in a mixture of odors.
- Identify the direction from which an odor is coming.
- Perceive the intensity of odors with great precision. This can allow them, for example, if two odors were left in similar conditions, to determine which of the two odors is the most intense, and therefore the most recent.

Detecting substances

An adversary can train detection dogs to detect the odors emitted by substances such as explosives, drugs, fire accelerants, or, less commonly, electronic devices. The adversary can use detection dogs:

- At an action site or during a **house raid (p. 72)** or **covert house visit (p. 15)** to determine if a substance is present and locate it.
- During an **ID check (p. 76)** to determine if the person being checked is carrying or has been in contact with a substance.

In many countries, the State uses detection dogs to detect illegal substances at borders, airports, train stations, etc.

Tracking people

When a person moves on foot, they leave behind an odor trail composed of:

- Their scent, including the odors emitted by water (sweat) and oil (sebum) secretions of their feet and by skin flakes falling from their body. Odors from sweat and sebum penetrate shoes, including rubber shoes.
- Odors of things stuck to the soles of their feet or shoes.
- If they wear clothes: odors of particles detaching from their clothes.
- If they wear shoes: odors of the materials the shoes are made of (rubber, leather, etc.)
- If they step on and break living plants, including grass: odors of sap released by broken plants and odors of bacteria breaking down dead parts of plants.
- If they step on and kill insects or other small animals: odors of the dead animals.

An adversary can train detection dogs to follow such an odor trail. There are two tracking methods:

- First method: The dog is provided with an odor, for example in the form of an item of clothing worn by a suspect, and is asked to locate and follow a trail that contains the odor. This method is more reliable.
- Second method: The dog is asked to locate and follow a trail without being provided with an odor. This method is less reliable.

In many countries, the State uses detection dogs to track suspects, but because dogs are not considered reliable, the result of the tracking is not considered strong evidence in court. In some countries, the result of tracking by the first method is considered strong evidence, but the result of tracking by the second method is not.

Detection dogs can often follow an odor trail up to two or three days after it was left, or even, depending on various factors, up to two or three months. Factors that affect the ability of a detection dog to follow a trail a long time after it was left include:

- The training of the dog and of its handler.

- Human activity on or near the trail.
- Wind. Air movement can displace the volatile chemical compounds that constitute a trail.
- Precipitations. Rain, snow or dew can dissolve some of the volatile chemical compounds that constitute a trail.

Scent lineups

An adversary can train detection dogs to participate in scent lineups. To set up a scent lineup, the adversary collects scent samples from a suspect and a few other people, typically between 5 and 10, and places the samples next to each other, typically in an empty room with some distance between two samples. The adversary then provides the dog with an odor and the dog is asked to determine which of the scent samples, if any, matches the odor. Typically, the dog is provided with an item collected at an action site that is suspected of carrying the suspect's scent: if the dog determines that the suspect's scent sample matches the item's odor, the adversary can conclude that the suspect was in contact with the item and may have participated in the action.

In countries where the State uses scent lineups, the result of a scent lineup is often not considered strong evidence in court.

See also

See the "Mantrailing" section of "How To Get Things Burning (Security Chapters)"[25] for an overview of detection dogs.

Mitigations

Careful action planning (p. 149): An adversary can use detection dogs to track you after an action. To mitigate this, when leaving the action site, you can plan to:

- Avoid leaving behind an item that carries your scent, which the adversary could provide to a dog to help the dog track you.

[25] https://notrace.how/resources/#things-burning

- Break your odor trail, for example by travelling a significant distance on a bike or crossing a large body of water.

Repressive operations

Fenix (p. 203): In one of the house raids, the police used detection dogs trained to detect explosives.[26]

Repression against Zündlumpen (p. 191): In some of the raids, detection dogs were used to locate electronic devices.[27]

Investigators made a covert visit of the cabins where N. and M. lived and, using handkerchiefs, collected scent samples from objects believed to belong to N. and M.[9] In the following months, on three occasions, after an arson took place in the region, they brought the handkerchiefs to the arson site and provided them to detection dogs, asking the dogs to locate the scents. The dogs signaled that they located the scents on the remains of firelighters, firelighter packaging, and a canister lid.

In the February 2025 arrests of N. and M., scent samples were collected from their necks.[28]

Bure criminal association case (p. 196): Detection dogs were used in one of the raids.[7]

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

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

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

3.6. Door knocks

Used in tactics: **Deterrence, Incrimination**

Door knocks are when an adversary comes knocking where you live to intimidate you or get information. Door knocks aim to intimidate or create paranoia, to see who is willing to talk and possibly be recruited as an **informant (p. 80)**, and to gather information from the people who do talk.

By logging who you call or visit immediately after they come knocking, the adversary can **map your network (p. 95)**.

In many countries, it is easier for the State to carry out door knocks than **house raids (p. 72)** because door knocks do not require a warrant or legal authorization.

Mitigations

Avoiding self-incrimination (p. 144): If an adversary knocks on your door, you can avoid talking to them: instead, alert your networks and consider making the event public.

Digital best practices (p. 152): You can follow digital best practices to make it harder for an adversary to log who you contact after they knock on your door.

Repressive operations

Search for a fugitive (p. 189): In 2025, agents from the Federal Bureau of Investigation (FBI) knocked on doors and asked for information about the person.[7]

Scintilla (p. 201): In May 2019, cops knocked on Boba's door under the pretext of giving a verbal notice to someone else.[29] Once inside, however, they revealed a warrant for Boba's arrest, arrested him, and searched the house.

3.7. Doxing

Used in tactic: **Deterrence**

Doxing is the practice of publishing a target's personal information without their consent in order to harm them or encourage others to harm them. It is most often used by non-State adversaries.

Doxing often uses information obtained through **open-source intelligence (p. 97)**.

Mitigations

Digital best practices (p. 152): You can follow digital best practices to make it harder for an adversary to dox you.

3.8. Evidence fabrication

Used in tactic: **Incrimination**

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

Notable examples of evidence fabrication include:

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

- Lying in a police report.
- Planting incriminating materials. For example, police in Baltimore (United States) were unaware that their body cameras continued to record after being turned off and recorded themselves planting drugs in a suspect's bag.

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

Mitigations

Physical intrusion detection (p. 170): An adversary often needs to covertly enter a space to plant evidence in the space. You can use physical intrusion detection to detect such a covert entry.

Repressive operations

Prometeo (p. 199): Investigators distorted conversations obtained through phone interception to make them look suspicious.[30] For example, during a phone conversation involving one of the defendants, the phrase "tutta questa tensione sociale prima o poi scoppierà" ("all this social tension will, sooner or later, explode") was said, which was only partially transcribed in the investigation files as "prima o poi scoppierà" ("will, sooner or later, explode").

December 8 case (p. 193): Investigators mistranscribed or distorted conversations obtained through phone interception or hidden microphones to make them look suspicious.[8] For example, the term "lunettes balistiques" (ballistic goggles) used in a conversation was transcribed as "gilets balistiques" (ballistic vests) by intelligence services, and became "gilets explosifs" (explosive vests) in a report by the prosecutors in charge of the case.

3.9. Forensics

Used in tactic: **Incrimination**

Forensics is the application of science to investigations for the collection, preservation, and analysis of evidence. It has a broad focus: DNA analysis,

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

fingerprint analysis, bloodstain pattern analysis, firearms examination and ballistics, toolmark analysis, serology, toxicology, hair and fiber analysis, footwear and tire tread analysis, drug chemistry, paint and glass analysis, linguistics, digital audio, video, and photographic analysis, etc.

In addition to linking a suspect's identity to an action, forensics is often used to link individual actions together.

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

3.9.1. Arson

A fire investigator searching the scene of a fire.

Arson forensics (also known as *fire investigation*) is the application of science to the investigation of arson. Arson forensics aims to determine the origin and cause of a fire and, if it is suspected to be arson, to gather evidence that could help identify the potential arsonists.

An adversary can usually easily determine whether a fire was accidental or arson. It is difficult to carry out an arson and make it appear accidental to an adversary who is knowledgeable in arson forensics.

Fire scene investigation

Fire scene investigation is the inspection of the scene of a fire, looking for:

- The ignition source that started the fire and the fuel that source ignited. For example, in an accidental residential fire the ignition

source may be a malfunctioning electrical outlet that overheats and the fuel may be a sofa positioned against the outlet. In an arson the ignition source may be a match and the fuel may be gasoline brought by the arsonist.

- Patterns left by the fire on walls, floors, ceilings, and objects. These patterns can indicate where the fire started and how it spread. For example, a fire that starts at the base of a wall may leave a distinctive V-shaped burn pattern on the wall.
- Eyewitness accounts and **video surveillance (p. 90)** footage of the scene of the fire before, during, and after the fire.

When a fire occurring inside a room reaches a high enough temperature —typically between 500°C and 600°C—it reaches the *flashover* point. During flashover, the room is so hot that all ignitable surfaces ignite more or less simultaneously and the fire spreads rapidly throughout the room. Once a fire has reached flashover it is usually significantly harder for the adversary to interpret the patterns it left on walls and other surfaces.

Fire debris analysis

Fire debris analysis is the collection and analysis of fire debris—objects that burned in a fire. An adversary can collect samples of fire debris at the scene of the fire and analyze them in a laboratory to find traces called ignitable liquid residues (ILRs), which are left when accelerants (also known as *ignitable liquids*) burn. An adversary can use **detection dogs (p. 26)** to locate ILRs at the scene of the fire, facilitating the collection of samples of fire debris that are likely to contain ILRs.

An adversary can analyze a sample of fire debris to determine:

- The presence of ILRs in the sample. This can indicate that the fire was arson rather than accidental and that the fire originated where the sample was collected.
- The type of accelerant that left the ILRs in the sample: gasoline, diesel fuel, kerosene, etc.

Accelerant comparison

An accelerant can have a more or less unique chemical composition depending on how it was produced, transported and stored. Let's take the example of gasoline, an accelerant made from refined crude oil. The chemical composition of gasoline sold at a gas station depends on:

- Where and how the crude oil was extracted.
- How the crude oil was refined.
- What chemicals were blended to make the gasoline.
- What additives were added to the gasoline. Additives can depend on the brand of gasoline, although a given brand can also use different additives depending on the region and the time of year.
- The chemical composition of the accelerant remaining at the bottom of the gas station's fuel tank when it was last refilled.[31]

An adversary can compare the chemical compositions of two samples of accelerant to determine the likelihood that they come from the same source. They can compare:

- An accelerant to an accelerant. This type of comparison is more precise. For example, they can compare a bottle of gasoline found unignited at the scene of a fire to gasoline found stored in a suspect's home.
- ILRs to an accelerant. This type of comparison is less precise. For example, they can compare ILRs from fire debris found at the scene of a fire to a sample of gasoline from a gas station.

If an adversary wants to know the source of a sample of accelerant—that we'll call the *questioned sample*—but does not have any particular leads, they have two options:

- They can collect a large number of potentially matching samples and compare them to the questioned sample. For example, they can collect gasoline samples from all gas stations in an area and compare them to a bottle of gasoline found unignited at the scene of a fire. State adversaries do not regularly do this.[32]

[31] Gas station fuel tanks are typically refilled every few days, or every few weeks at stations with fewer customers.

- If they have access to an *accelerant database*—a database of samples of accelerants collected regularly in a given region—they can compare the questioned sample to all the samples in the database. For example, if the questioned sample is a bottle of gasoline found unignited at the scene of a fire, they could identify the brand of gasoline (if samples are collected from refineries whenever a batch of gasoline is produced for a given brand) or the gas station where it was bought (if samples are collected from gas stations whenever their fuel tanks are refilled). It is unknown if any State adversaries have access to such databases.[33]

Incendiary devices

An incendiary device is an arrangement of items or materials that is designed to be left at the scene of a fire in order to help start, accelerate, spread, or delay the fire. Incendiary devices range from simple Molotov cocktails to complex time-delay devices with electronic timers.

Since incendiary devices are designed to be left at the scene of a fire, an adversary can recover their burned remains and analyze them to find evidence that could help identify the arsonists. It is relatively common for incendiary devices to fail—whether they fail to ignite or ignite but burn significantly less than expected—in which case an adversary can recover the devices intact or partially intact and potentially find much more evidence than if the devices had not failed.

Incendiary devices can fail because of:

- An inherent flaw in the construction or use of the device. For example, Molotov cocktails typically have a high failure rate because they often either do not break upon contact with their target, or break but fail to sufficiently ignite their target.
- Rough handling of the device during construction, transport, or installation. This rough handling can be caused by stress, darkness, or inexperience.

[32] According to a 2023 study from the United States, this is "not common practice in forensic casework."

[33] A 2020 study from the Netherlands briefly mentions "a database of gasoline collected nationally."

- Weather conditions during storage of the device (between its construction and use), particularly if it includes moisture-sensitive components.
- Weather conditions at the scene of the fire: wind, dew, fog, and rain.

When analyzing an incendiary device or its burned or partially burned remains, an adversary can analyze:

- Accelerants contained in the device, or ILRs left on the device.
- **DNA traces (p. 42)** and **fingerprints (p. 53)** left while handling the device components.
- **Tool marks (p. 64)** left when constructing the device.
- Identifiers visible on the device components such as serial numbers or barcodes.
- **Glass traces (p. 64)**, if the device includes glass components.
- Details of the device's construction, including the use of tape and glue and how components are wired, welded, or knotted together.

An adversary may successfully analyze a DNA trace left on an incendiary device even if the device ignited, depending on the type of trace, the temperature to which it was exposed, and the duration of the exposure.[34] For example:

- A saliva trace was left on the outside of a Molotov cocktail made from a glass bottle. The Molotov cocktail was thrown and broke but only produced a short-lived burst of flames without further damage. An adversary may successfully analyze the DNA in the saliva trace.
- Skin cells were left on the outside of an incendiary device. The device was activated and surrounding objects caught fire, resulting in a sustained fire that enveloped the device for several minutes. An adversary should not be able to successfully analyze the DNA in the skin cells.

[34] For more information see the "Degradation" section of the No Trace Project DNA Literature Review.[a]

[a] https://notrace.how/resources/#dna-review

See "Incendiary Devices: Investigation and Analysis",[35] chapter "The Analysis of Incendiary Devices" for a detailed overview of the investigation of incendiary devices.

Mitigations

Anonymous purchases (p. 139): An adversary can link accelerants and incendiary device components to where they were purchased, and from there to the identity of the person who purchased them. To mitigate this, you can purchase accelerants[36] and device components anonymously.

Careful action planning (p. 149): If you use an incendiary device in an action and the device fails, an adversary can recover the device intact or partially intact and potentially find much more evidence than if the device had not failed. To mitigate this, you can:

- Make and use several test devices similar to the "real" device you will use in the action. You should conduct the tests with good security precautions because conducting such tests can be incriminating. In particular, you can:
  - Construct test devices with components of the same brand and model as the components you will use for the real device.
  - Store test devices in the same conditions (e.g. humidity) as the real device, and for the same length of time.
  - Transport test devices in the same way as the real device.
  - Install test devices in the same conditions as the real device (weather, temperature, darkness, etc.)
- Ensure that you will be able to construct, transport, and install the device under the psychological conditions of the action (e.g. stress).

If you use accelerant in an action and an adversary goes through the effort of collecting accelerant samples for comparison (e.g. gasoline samples

[35] Available on the Surveillance Archive.[a]

[a] https://notrace.how/surveillance-archive.html

[36] If it is too difficult to purchase accelerants anonymously in your context (e.g. because it is too suspicious to buy gasoline from a gas station without arriving in a car), you can prefer to purchase them non-anonymously, and mitigate this technique in other ways.

from gas stations), they could identify the source of the accelerant you used. To mitigate this, you can:

- Make the identification less likely to be effective by using a mix of accelerants of the same type coming from different sources (e.g. gasoline from different gas stations).
- Make the identification even less likely to be effective by using a mix of accelerants of the same type from sources located in different areas (so that the chemical compositions of the accelerants are more distinct) and let some time pass between when you obtain the accelerants and when you use them (so that the adversary cannot retroactively obtain the samples they would need for comparison because the fuel tanks of the gas stations where you obtained the accelerants have been refilled).

Repressive operations

Mauvaises intentions (p. 208): DNA samples were collected from a cigarette used as a delay for an incendiary device—the delay failed and the device was found intact under the police tow truck.[37]

Case against Louna (p. 182): A gas detector[38] was unsuccessfully used to detect traces of accelerant in the cab of the burned excavator.[7]

Traces of accelerant were collected:

- On a torch—a piece of wood tipped with a cloth soaked in flammable liquid—found near the burned excavator.
- Inside the burned excavator.

Traces of accelerant were unsuccessfully searched for on Louna's clothes, seized at the hospital while she was hospitalized.

Repression of the first Jane's Revenge arson (p. 185): DNA samples were collected from an intact Molotov cocktail found by investigators at the action site.[39]

---

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

[38] https://en.wikipedia.org/wiki/Gas_detector

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

Bure criminal association case (p. 196): Traces of accelerants were collected from items recovered after demonstrations and analyzed.[7]

3.9.2. Ballistics

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

Ballistic forensics (also known as *firearm examination*) is the application of science to the investigation of firearms and bullets. When a bullet is fired from a gun, the gun leaves microscopic marks on the bullet and cartridge case. These marks are like ballistic fingerprints.

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

Mitigations

Anonymous purchases (p. 139): An adversary can use ballistic forensics to trace back a firearm or bullet to a seller, and from there to the identity of the person who purchased the firearm or bullet. To mitigate this, you can purchase firearms and bullets anonymously, for example through connections to organized criminal networks or through fraud.

Stash spot or safe house (p. 174): An adversary needs to have access to a firearm to perform a ballistic analysis on the firearm. To prevent this, you can store the firearm in a stash spot or safe house.

3.9.3. DNA

Collection of a DNA sample using a swab.

DNA forensics is the collection and analysis of DNA samples for the purpose of matching DNA samples to individuals.

DNA is the molecule that contains the genetic code of organisms. Every cell[40] in a human body has DNA. Each individual's DNA is unique, with the exception of identical twins. An adversary can compare an individual's DNA with a DNA sample collected from an item or location and, if they match, conclude that the individual was likely in contact with that item or location.

Transfer

Human body cells and the DNA they contain can directly transfer from the body to the environment. For example:

- When you sweat, urinate, defecate, or bleed, you leave sweat, urine, feces, or blood.
- When you breathe or speak, you emit respiratory droplets from your mouth and nose that contain saliva and mucus.
- When you touch a surface with your skin, skin cells transfer from your skin to the surface.

[40]With the exception of red blood cells.

- Even when you're not doing anything, you are constantly shedding skin cells and hair.

Human body cells can also transfer indirectly. For example, if you touch the outside of a pair of gloves with your fingers, then put the gloves on and touch a door handle, your skin cells can transfer first from your fingers to the outside of the gloves and then from the outside of the gloves to the door handle.

See the "Transfer" section of the No Trace Project DNA Literature Review[41] for more details on direct and indirect DNA transfer.

Degradation

DNA is very robust and does not easily degrade, but it can degrade under certain conditions, such as when exposed to high temperatures or sodium hypochlorite.

See the "Degradation" section of the No Trace Project DNA Literature Review[41] on the conditions under which DNA can degrade.

Collection

An adversary can collect a DNA sample:

- From a surface known to contain DNA, such as a visible biological mark (e.g. saliva or blood).
- From a surface suspected of containing DNA, such as a door handle suspected to have been touched by a suspect at an action site.

An adversary can use techniques to facilitate DNA collection, such as:

- Soot removal techniques to collect DNA samples hidden beneath soot after a fire.
- Luminol to locate blood samples invisible to the naked eye.

Analysis

An adversary can analyze a DNA sample to identify genetic markers of the DNA. Such an analysis is successful if:

[41] https://notrace.how/resources/#dna-review

- The sample contains enough DNA. For example, a drop of blood contains significantly more DNA than skin cells left through brief contact between skin and a surface.
- The DNA isn't too degraded.
- All or most of the DNA in the sample is from at most three individuals.

An adversary can compare *two* successfully analyzed DNA samples to:

- Determine whether they come from the same individual. For example, they can compare a DNA sample collected from the mouth of a suspect in custody to a DNA sample collected at an action site and, if they match, conclude that the suspect was likely present at the action site.
- Determine whether they come from individuals closely related genetically, such as parents and their children, siblings, or cousins.

An adversary can also use a *single* successfully analyzed DNA sample to:

- Determine the individual's genetic sex.
- Attempt to predict the individual's appearance using forensic DNA phenotyping. Currently, eye, hair, and skin color can be predicted with relatively high accuracy, and research is ongoing to attempt to predict other characteristics. This technique is not used in all contexts.

DNA databases

In many countries, the State has DNA databases containing the DNA of many individuals, often obtained during arrests or as part of criminal convictions.

Countries can exchange DNA data with each other through:

- International DNA databases, such as the Interpol DNA database or the Europol Information System.
- Linked or networked national DNA databases. For example, European Union member states are required to maintain a DNA database that other member states can access.
- Request-based exchange of DNA data, typically in cases of serious crimes.

See also

- Dna You Say? Burn Everything to Burn Longer: A Guide to Leaving No Traces[42] for an overview of DNA forensics.
- The No Trace Project DNA Literature Review[41] for a collection of useful details on DNA forensics, taken from academic literature.
- The "DNA" topic.[43]

Mitigations

Careful action planning (p. 149): An adversary can use DNA forensics to collect DNA at an action site. To mitigate this, you can carefully plan the action to minimize DNA traces at the action site. For example, you can:

- Secure your hair under a hat.
- If you have to cut a fence, cut any fence holes large enough to pass through without touching the fence.
- Ensure that surfaces at the action site are not touched if they do not need to be, and that surfaces that need to be interacted with (such as a door handle) are touched by someone following **DNA minimization protocols (p. 160)**.
- Ensure that nothing is accidentally left behind such as a bag, tool, or anything that could fall out of a pocket.

DNA minimization protocols (p. 160): You can minimize the amount of DNA you leave on a surface to minimize the risk that an adversary can use DNA forensics to draw a valuable conclusion from an analysis of the surface.

Gloves (p. 163): You can wear gloves to avoid leaving DNA on surfaces you touch.

Repressive operations

Scripta Manent (p. 210): DNA evidence was used to convict Alfredo

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

Cospito.[44]

Case against Boris (p. 188): The only evidence against Boris was that his DNA was found on a bottle cap at the foot of one of the burnt antennas from the April sabotage.[22]

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

2019-2020 case against Mónica and Francisco (p. 190): Francisco's DNA was found on the parcel bomb sent to the former Minister of the Interior, which was defused and didn't explode.[45]

Repression against Zündlumpen (p. 191): In some of the raids, DNA samples were collected from a cigarette butt,[46] zines,[47] books, doors, cups, and printing machines.

Renata (p. 200): After their arrest and imprisonment, the person accused of the explosive attack on the Lega Nord headquarters in Treviso refused to have their DNA taken.[48] Some time after the person's refusal, prison guards searched their cell and secretly replaced one comb with another, presumably to obtain the person's DNA from the hairs on the comb they took.

Search for a fugitive (p. 189): Following the 2020 attack on the building, DNA samples were collected from broken glass, window blinds, the sidewalk outside the building, as well as on blood found on a bottle of lighter fluid and other items.[7] It seems that at this point, the samples did not match anyone in DNA databases.

---

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

[45]https://notrace.how/resources/#monica-francisco

[46]https://notrace.how/resources/#bavarian-christian

[47]https://notrace.how/resources/#cops-and-robbers

[48]https://web.archive.org/web/20210518112509/https://roundrobin.info/2020/03/aggiornamenti-su-manu-stecco-juan-e-sasha

In 2023, the person was convicted in an unrelated case in a state other than Georgia. As part of the conviction, they were required to provide a DNA sample to the police, which matched the samples collected in 2020.

Repression of Lafarge factory sabotage (p. 185): In one of the initial raids, police insisted that those arrested wear surgical masks to protect against Covid: the masks were later taken for DNA collection.[49] One person who refused to wear a mask had their underwear confiscated while in police custody, presumably for DNA collection.[50]

Prometeo (p. 199): DNA traces were used to convict the person accused of burning an ATM.[51]

Mauvaises intentions (p. 208): During police custody, DNA was collected from the people's clothing and from plastic cups.[37] In one case, only nine hours elapsed between the collection of a DNA sample in custody and the result of its comparison with another sample collected earlier.

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

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

Case against Amos Mbedzi (p. 207): Mbedzi's DNA was found on a cushion and a sun visor of the car used to transport the explosive device to the bombing site.[52]

Case against Louna (p. 182): DNA samples matching Louna's DNA were collected from:[7]

---

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

[50]https://notrace.how/resources/#lafarge

[51]https://web.archive.org/web/20210612231740/https://roundrobin.info/2021/05/sentenza-beppe

[52]https://notrace.how/documentation/case-against-amos-mbedzi-case-file.pdf

- A garbage bag and a surgical mask, partially burned, seized near the burned excavator.
- A pair of shorts seized in her hospital room while she was hospitalized.
- A paper cup seized when she was taken into custody.
- A spoon and a napkin seized while she was in custody, after a meal.

DNA samples matching the DNA a person seen asking after Louna in the corridors of the hospital were collected from:

- A pair of shorts seized in Louna's hospital room while she was hospitalized.
- A surgical mask found in the shorts.

Unusable DNA samples were collected from:

- A partially burned hammer found in the cab of the burned excavator, the window of which had been broken.
- A torch—a piece of wood tipped with a cloth soaked in flammable liquid—found near the burned excavator.

Repression of the first Jane's Revenge arson (p. 185): In May 2022, DNA samples were collected from several items found by investigators at the action site, including a broken window, a glass jar, a lighter, and an intact Molotov cocktail.[39] In March 2023, police saw the person discard a bag containing a partially eaten burrito in a public trash can. DNA samples collected from the bag's contents matched those collected at the action site.

Scintilla (p. 201): The charge against Peppe was based on a match between DNA traces found inside the parcel bomb and his DNA collected from a cigarette butt during the investigation.[53]

Bure criminal association case (p. 196): DNA samples were collected from:[7]

- Items recovered after demonstrations, including fireworks, Molotov cocktails, a lighter, and rocks used to break windows.
- Items found during raids, including clothing, gas masks, helmets, and containers filled with gasoline or other substances.

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

Investigators were unable to match the vast majority of the DNA samples they collected to anyone. Notable exceptions were:

- A DNA sample collected from a Molotov cocktail found in a raid matched an individual in the national DNA database.
- A DNA sample collected from the lid of a jar containing materials that could be used to build explosive devices, found in a raid, matched an individual in the national DNA database.
- A DNA sample collected from a lighter recovered after a demonstration matched another trace from an earlier, unrelated case, but did not match anyone in the national DNA database.

Case against Ruslan Siddiqi (p. 184): DNA samples were collected from people living in a large area surrounding the train bombing site, including from soldiers and Ukrainian citizens, presumably because they were deemed potential suspects.[54]

Nea Filadelphia case (p. 207): The charges against several people were based on a match between their DNA, taken by force while in custody, and DNA samples collected from "mobile objects" near the robberies.[55]

Panico (p. 198): DNA traces were the only evidence against one of the defendants.[56]

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

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

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

3.9.4. Digital

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

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

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

Mitigations

Avoiding self-incrimination (p. 144): An adversary can use digital forensics to retrieve self-incriminating information from a digital device. To mitigate this, you can avoid storing such information on digital devices except for very deliberate reasons (such as writing and sending an action claim while following **digital best practices (p. 152)**).

Digital best practices (p. 152): An adversary can use digital forensics to retrieve data from a digital device you have used. To mitigate this, you can follow digital best practices and, in particular, use Tails,[57] an "amnesic" operating system designed to leave no trace on the computer it runs on.

[57] https://tails.net

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

- Use popular rather than custom tools.
- If you use a Virtual Private Server (VPS), **purchase it anonymously (p. 139)** and access it through Tails.[57]

Encryption (p. 161): An adversary can use digital forensics to retrieve data from unencrypted digital devices. To mitigate this, you can encrypt your digital devices with Full Disk Encryption and a strong password.

Metadata erasure and resistance (p. 166): An adversary can use digital forensics to retrieve and analyze metadata. To mitigate this, you can erase metadata from files before publishing them online or sending them to others.

Repressive operations

Case against Revolutionära fronten (p. 204): Investigators analyzed the computer of one of the defendants, that was seized during a raid, and retrieved messages sent and received by the defendant on the messaging application MSN Messenger.[7] The messages included:

- Detailed discussion of the Stockholm beating, including mentions of the names of some of the defendants as participants in the beating.
- Discussion of the nighttime visit to the fascist's house, including mentions of the names of the occupants of the house and mentions of the names of some of the defendants as participants in the visit.

Bure criminal association case (p. 196): Investigators analyzed storage devices by automatically extracting files containing the following keywords relevant to the investigation:[7]

- "*Action*".
- "Andra", the agency responsible for the Cigéo project.
- "Bindeuil", the name of the building that was attacked during the June 21, 2017 demonstration.

- "*Hibou*" ("owl"), a name used by people fighting against Cigéo to refer to themselves.
- "*Incendie*" ("fire").

3.9.5. Facial recognition

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

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

Modern facial recognition systems are capable of matching a face image against a large database of faces, even if the face in the image is masked, with only the eyes and eyebrows visible. Facial recognition systems coupled with **mass video surveillance (p. 90)** can be used to automate the tracking of individuals through a space.

See the "Facial recognition" topic.[58]

Mitigations

Anonymous dress (p. 137): You can wear a mask that adequately covers your face, including your eyebrows and up to the top of your nose.

Biometric concealment (p. 147): You can wear a mask to cover your facial features, and sunglasses or a hat with a low brim to cover your eyes.

Repressive operations

2019-2020 case against Mónica and Francisco (p. 190): In order to identify Mónica and Francisco on public CCTV footage, photos of both were compared to the footage, including a comparison of several facial features: eye distances, wrinkles, piercing scars, ear size, mouth and nose shape.[45]

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

2013 case against Mónica and Francisco (p. 204): The main evidence against Mónica and Francisco was a comparison of photos of both of them with public CCTV footage that showed their uncovered faces while they were in the subway, shortly before or after the action.[59]

Repression of the attack on Clarín's headquarters (p. 187): Investigators used facial recognition software to identify one of the defendants, using a photo of their face extracted from CCTV footage near the attack site.[60]

3.9.6. Fingerprints

Ridges on a human finger.

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

Collection

Fingerprints are left on surfaces you touch by the moisture and grease on your fingers, and can be collected from these surfaces. They can also be collected directly from your fingers using ink or other substances (fingers are first dipped in ink, then put on paper, leaving impressions on the paper), or using electronic fingerprint scanners.

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

Analysis

Because fingerprints are nearly unique and durable over the life of an individual, two fingerprints can be compared to determine if they belong to the same individual.

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

Fingerprint databases

In many countries, the State has fingerprint databases containing the fingerprints of many individuals, often obtained during arrests or as part of criminal convictions.

Other types of prints

Human palms and toes can leave impressions similar to fingerprints, which can be collected and analyzed in the same way. In some contexts, palm prints are regularly collected and added to fingerprint databases.

See also

See the "Fingerprints" topic.[61]

Mitigations

Careful action planning (p. 149): An adversary can use fingerprint forensics to collect and analyze fingerprints at an action site. To mitigate this, you can carefully plan the action so that any tools you plan to use during the action are free of fingerprints in case you lose them or have to discard them in a location where they can be recovered by an adversary.

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

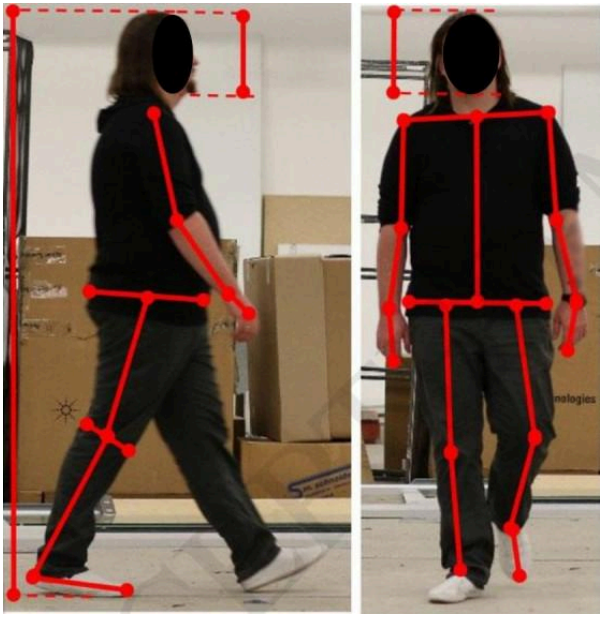
Gloves (p. 163): You can wear gloves to avoid leaving fingerprints on surfaces you touch.

Repressive operations

Bure criminal association case (p. 196): Fingerprints were collected from items found during raids, including a notebook, sheets of paper, gas masks, helmets, Molotov cocktails, and containers filled with gasoline or other substances.[7] The vast majority of the fingerprints collected did not match anyone. Some of the fingerprints collected matched individuals in the national fingerprint database.

Repression of the attack on Clarín's headquarters (p. 187): The fingerprints of one defendant were found on a Molotov cocktail that was used in the attack but did not break.[60]

3.9.7. Gait recognition



Left: a person walking, seen from the side. Right: the same person walking, seen from the front. Red lines mark some of the body features used for gait recognition.

Gait recognition (also known as *gait analysis*) is the analysis of the manner or style in which people move for the purpose of matching one manner or style to another.

Factors of gait

When you move, you naturally adopt a relatively unique gait that depends on several factors, including:

- Intrinsic factors: how you learned to walk, your anatomy and physiology, and any injuries or pathologies you may have.
- Extrinsic factors: your clothing and the terrain on which you move (flat or not, with or without obstacles…)

Analysis

An adversary watching you move can locate, measure, and categorize your body features (position of your ankles, knees, hips…) at various stages of movement and compare them to the body features of another moving person. This comparison can allow the adversary to determine whether or not you could be that other person, but it usually doesn't allow the adversary to determine with certainty that you are that other person. This comparison is usually done by humans, sometimes assisted by specialized software.

Gait recognition is typically done by comparing two sets of video footage. The first set shows a first person moving, and the second set shows a second person moving. The goal of the comparison is to determine whether or not the first and second person could be the same person. The strength of the recognition, that is, the confidence in the determination that the first person could be the second person or not, depends on several factors, including:

- The quality and frame rate of the footage.
- The lighting in the scene.
- Whether the two people are sufficiently close to the camera, fully visible, taking several steps, and wearing clothing that doesn't excessively hide their gait.

- Whether the two people have a generic or unique gait. For example, a person with a limp has a rather unique gait.
- Whether the two people are seen from similar angles performing the same type of movement (e.g. either walking or running).

Typical scenario

The following is a typical scenario in which an adversary uses gait recognition:

- A person is captured by CCTV carrying out an action. They are not recognizable because they are **dressed anonymously (p. 137)**. The adversary obtains the CCTV footage.
- Based on other evidence, the adversary suspects someone of having carried out the action. They obtain footage of this suspect moving, either through CCTV near their home, CCTV while they are in custody, or a **covert video surveillance device (p. 23)**.
- The adversary compares the person's gait in the first footage to the suspect's gait in the second footage to determine whether or not they could be the same person, and the confidence in that determination.

See also

See Forensic Gait Analysis: Principles and Practice[35] for a comprehensive overview of gait recognition.

Mitigations

Anonymous dress (p. 137): You can wear baggy clothing to conceal your gait.

Biometric concealment (p. 147): You can wear baggy clothing that hides your body shape, use an umbrella or other concealing objects, or drastically change your walking style by adopting a "funny walk".

Careful action planning (p. 149): An adversary can use gait recognition to analyze your gait on CCTV footage at or near an action site. To mitigate this, you can carefully plan the action so you avoid moving with your usual gait near a camera.

Bialystok (p. 195): The main evidence against the person accused of an explosive attack on a police station was a comparison of his gait and the color of his coat with the corresponding characteristics of a person recorded by the surveillance cameras of the police station.[62]

Scintilla (p. 201): Two of the people were accused of arson because their gait and body shapes were considered compatible with people recorded by video surveillance cameras placing a canister of flammable liquid in front of an Italian post office.[63]

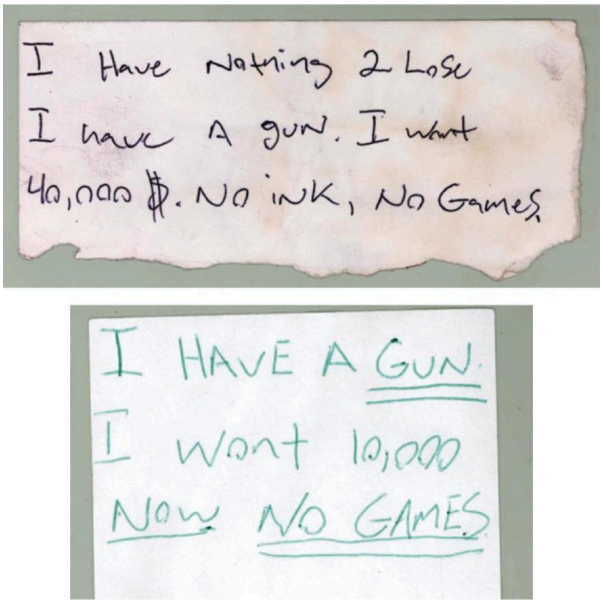
Operation 8 (p. 209): One person was identified in footage of the "training camps" based on their height, gait, and skin color.[7]

Repression of the attack on Clarín's headquarters (p. 187): One of the defendants was identified because their gait was considered compatible with that of a suspect visible in CCTV footage near the attack site.[60]

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

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

3.9.8. Handwriting analysis



Two robbery notes[64] showing similarities in the formation of the number "0".

Handwriting analysis (also known as *handwriting recognition*) is the analysis of handwriting samples, typically for the purpose of matching one sample to another.

Factors of handwriting

When you write, you naturally adopt a relatively unique handwriting that depends on several factors, including:

- How you learned to write: how you learned to form letters and move the writing instrument.
- Your writing habits: how you personally form letters and move the writing instrument, which can be more or less similar to how you learned.

[64] Some bank robberies are carried out by discreetly handing the teller a written note demanding money in order to draw as little attention as possible.

- Your writing level: whether you are learning to write or are an experienced writer.
- The writing instrument: pen, pencil, brush, spray paint can, etc.
- Where you hold the writing instrument: in your right hand, left hand, foot, mouth, prosthesis, etc.
- How you hold the writing instrument: for example, on which of your fingers does a pen rest when you write.
- The writing surface: paper, fabric, concrete, etc.
- Your posture while writing: sitting, standing, etc.
- The writing environment: for example, if you are writing with gloves on or in a moving vehicle.
- Your physical and mental state while writing: fatigue, stress, altered state due to alcohol, drugs or medication, etc.

Analysis

An adversary can analyze a writing sample to identify its characteristics, including:

- The layout of the text: margins, space between lines, and parallelism of lines. In the case of envelopes: the style, size, and position of the address on the envelope.
- The writing style: for example cursive or block letters.
- The space between characters and between words.
- Connections or separations between characters.
- The design and construction of characters: the shape of characters, whether a character is represented with one or more shapes throughout the sample, the order in which a shape is traced, whether and how a shape is affected by the particular shapes that precede and follow it, and the size of shapes.
- The strokes traced when the writing instrument reaches and leaves the writing surface, including their length, direction, path, and abruptness.
- The pressure exerted by the writing instrument on the writing surface.
- The position of the writing instrument relative to the writing surface.

In some languages that are written horizontally, such as English, an adversary can also identify the following characteristics:

- Whether the baseline[65] is straight or varies throughout the sample.
- The writing slant: the predominant inclination of characters relative to the baseline.

An adversary can compare the characteristics of a writing sample to the characteristics of another to determine whether or not the samples were written by the same person, and the confidence in that determination. This comparison can be done by humans or by specialized software.

Handwriting databases

In some countries, the State has databases of handwriting samples that allow comparing a sample to all samples in the database. For example, in the United States, the Federal Bureau of Investigation (FBI) maintains the Bank Robbery Note File (BRNF), which contains samples of handwritten notes used in bank robberies.

See also

See also Huber and Headrick's Handwriting Identification: Facts and Fundamentals[35] for a comprehensive overview of handwriting analysis.

Mitigations

Biometric concealment (p. 147): An adversary can identify the characteristics of a writing sample to identify its author. To mitigate this, if you are writing an incriminating text and you want to conceal your handwriting:

- If you don't need to hide that you are concealing your handwriting, you can take as many of the following measures as possible:
    - Hold the writing instrument in an unusual way. For example, if you normally hold a pen in your right hand, hold it in your left hand instead.

[65] The baseline is the horizontal line upon which the characters "sit". For example, the "loop" of a lowercase "p" sits on the baseline, while its "tail" extends below the baseline.

    - Use a writing style that produces generic rather than unique characters. For example, use uppercase block letters rather than cursive.
    - Pause for a few seconds between each character to avoid unconsciously falling back into your writing habits.
    - Keep the text as short as possible.
- If you need to hide that you are concealing your handwriting, you can use a handwriting that looks natural but does not feature the characteristics of your normal handwriting. This is difficult and may take years of practice.

Repressive operations

Scripta Manent (p. 210): Handwriting samples of some of the defendants (including notes seized during raids and letters written from prison) were compared to handwritten addresses on unexploded parcel bombs in an attempt to link the defendants to the attacks.[66]

2019-2020 case against Mónica and Francisco (p. 190): The labels on the two parcel bombs remained intact—one because the parcel didn't explode, and one despite the explosion of the parcel.[45] The handwritten signatures on the labels were compared and positively matched. This showed that the parcels were sent by the same person.

Repression of the first Jane's Revenge arson (p. 185): A comparison between the cursive graffiti left at the action site and the same style of graffiti painted a few months later during a demonstration helped identify the person.[39]

3.9.9. Linguistics

Forensic linguistics is the application of linguistic knowledge to identify the author of a text or the person behind a voice. Author identification (also called *stylometry*) is based on the analysis of certain patterns of language

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

use: vocabulary, collocations, spelling, grammar, etc. Voice identification is based on speech sounds (*phonetics*) and the acoustic qualities of the voice.

Author identification

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

- Who wrote an anonymous action claim posted on the Internet or sent to a newspaper.
- Whether multiple anonymous action claims were likely written by the same person or group.
- Who wrote a plan describing illegal activities found during a **house raid (p. 72)**, a **covert house visit (p. 15)** or an arrest.

Voice identification

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

- Who is speaking on a tapped mobile phone or a recording made by a **hidden microphone (p. 18)**.
- Who called the authorities to make a bomb threat.

See also

On the topic of author identification:

- Counteracting Forensic Linguistics.[67]
- Who wrote that?[68]

Mitigations

Biometric concealment (p. 147): You can hide the acoustic properties of your voice to mitigate voice identification.

Masking your writing style (p. 165): You can mask your writing style to mitigate author identification.

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

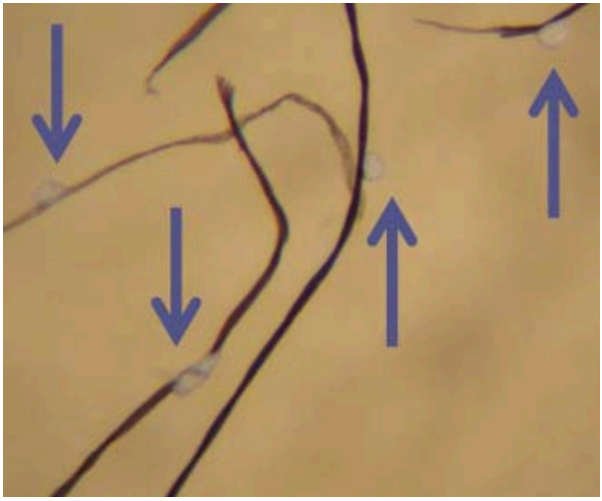
[68] https://notrace.how/resources/#who-wrote

Scripta Manent (p. 210): Texts published by some of the defendants were compared with action claims by the Informal Anarchist Federation, with the aim of proving that the defendants had written these claims.[66]

Repression against Zündlumpen (p. 191): Investigators compared texts from the newspaper Zündlumpen with private letters found in house raids, hoping to prove that people had written in the newspaper.[47]

Case against Direct Action (p. 212): Investigators noticed linguistic similarities between action claims published by Direct Action and articles in a local quarterly publication called Resistance.[11] This led them to identify a contributor to Resistance, who was a friend of members of Direct Action, and place her under **physical surveillance (p. 99)**.

3.9.10. Trace evidence



Spray paint droplets adhering to the fibers of a jacket, observed under a microscope (magnification ~75x). When spraying from a spray paint can, paint droplets from the resulting mist are likely to fall on nearby surfaces.

Trace evidence is the small fragments of physical evidence that are transferred between objects, people, and the environment. Trace evidence

can be collected and analyzed to establish links between objects, people, and places.

Trace evidence can be:

- Fragments of matter. For example, mud on the sole of a shoe or shards of glass from a broken window.
- Impressions left when two surfaces come into contact. For example, a shoeprint in the mud or a cut made by a bolt cutter in a fence.

Trace evidence can be transferred:

- With contact. For example, clothing touches a fence and fibers from the clothing transfer to the fence.
- Without contact. For example, a window is broken and shards of glass fly away and transfer to the clothing of people nearby.
- Through a chain of transfers, with and/or without contact.

An adversary can use trace evidence to:

- Analyze a trace from an action site to obtain useful information. For example, they can analyze a shoeprint found at an action site to determine the size and model of the shoe that left it, and then search for people who possess shoes of that size and model.
- Link a trace from an action site to an object. For example, they can determine whether textile fibers found on a fence at an action site likely come from clothing that they seized from your home during a **house raid (p. 72)**.
- Link a trace from an object to an action site. For example, they can determine whether shards of glass found on your clothing during your arrest likely come from a window that was recently broken nearby.
- Link traces from different action sites. For example, they can determine whether hammer marks found at different action sites were left by the same hammer, and therefore the actions were likely carried out by the same people.

Trace evidence does not include **fingerprints (p. 53)** and **DNA (p. 42)**, which are considered separate forensic disciplines.

Fibers

When an object made of textile fibers—clothing, a bag, etc.—touches a surface, it can leave fibers on the surface. The likelihood that an object leaves fibers on a surface and the amount of fibers left depend on the object, the surface, and the duration and type of contact between the two.

An object made of textile fibers can leave more or less unique fibers, depending on the object and its manufacturing process. For example:

- A worn wool sweater of an uncommon color, manufactured in an uncommon way, may leave a large amount of relatively unique fibers.
- A new nylon windbreaker of a common color, manufactured in a common way, may not leave any fibers, or only very generic ones.

An adversary can:

- Analyze fibers to determine the type of object that left them and, in some cases, its make and model.
- Compare fibers to an object in their possession to determine if the object could have left the fibers.
- Compare two sets of fibers to determine if they could have been left by the same object.

See Handbook of Trace Evidence Analysis,[35] chapter "Fibers" for an overview of fibers.

Footprints

When you are barefoot and your feet touch a surface, you can leave footprints on the surface. You usually leave footprints on the insoles of the shoes you wear. You can leave footprints when you are wearing socks.

A foot can leave a more or less unique print, depending on the foot and the surface. For example:

- On a hard, dusty surface, a foot may leave a very unique footprint that shows the ridges of the toes, which are as unique as **fingerprints (p. 53)**.
- On a soft surface such as sand, a foot may leave a very generic footprint that shows only a rough outline of the foot.

An adversary can:

- Analyze a footprint to obtain information about the person who left it, such as the size of their feet, an estimate of their height, and what they were doing when they left the footprint—standing, walking, running, turning around, etc.
- Compare a footprint to a foot to determine if the foot left the footprint.
- Compare two footprints to determine if they were left by the same foot.

See Examination and Interpretation of Bare Footprints in Forensic Investigations[69] for an overview of footprints.

Shoeprints

When you wear shoes and your feet touch a surface, you can leave shoeprints on the surface.

A shoe can leave a more or less unique print, depending on the shoe and the surface. Even mass-produced shoes of the same model vary slightly due to irregularities in the manufacturing process and to wear patterns. For example:

- On a clean wooden floor, a worn, dirty shoe may leave a very unique print.
- On a carpet, a new, clean, dry shoe may not leave a print, or only a very generic one.

An adversary can:

- Analyze a shoeprint to determine the size and model of the shoe and to obtain information about the person who left it, such as the size of their feet and an estimate of their height.
- Compare a shoeprint to a shoe in their possession to determine if the shoe left the shoeprint. To do this, they can use the shoe to make reference prints and compare them to the suspect shoeprint.
- Compare two shoeprints to determine if they were left by the same shoe.

[69] https://notrace.how/documentation/examination-and-interpretation-of-bare-footprints-in-forensic-investigations.pdf

See Footwear Impression Evidence: Detection, Recovery and Examination[35] for a comprehensive overview of shoeprints.

Tool marks

Tools—bolt cutters, scissors, hammers, screwdrivers, etc.—can leave marks on the objects they are used on.

A tool can leave a more or less unique mark, depending on the tool, how it is used, and on the surface. Even mass-produced tools of the same model vary slightly due to irregularities in the manufacturing process and to wear patterns. For example:

- A worn metal hammer used to forcefully strike a metal plate made of a softer metal may leave a very unique mark.
- A brand new bolt cutter used to cut a fence may leave a relatively generic mark.

An adversary can:

- Analyze a mark to determine the type of tool that left it.
- Compare a mark to a tool in their possession to determine if the tool left the mark. To do this, they can use the tool to create reference marks and compare them to the suspect mark.
- Compare two marks to determine if they were left by the same tool.

See also:

- PRISMA,[70] section "Tool Traces" for a short discussion of tool marks.
- Color Atlas of Forensic Toolmark Identification[35] for a comprehensive overview of tool marks.

Glass

When glass breaks, it produces shards of various sizes.

A glass object (e.g. a window, a bottle) produces more or less unique shards when broken, depending on how, where and when it was manufactured. For example:

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

- Two glass objects of different models, or manufactured in different factories, or manufactured in the same factory several weeks apart, may produce shards that can be distinguished by analyzing their properties, including their refractive indices[71] and chemical elements.[72]
- Two glass objects of the same model, manufactured in the same factory during the same week, may produce shards that are indistinguishable.

An adversary can compare two shards of glass to determine the likelihood that they come from the same object.

See Handbook of Trace Evidence Analysis,[35] chapter "Interpretation of Glass Evidence" for an overview of glass evidence.

Traces of accelerant

Traces of accelerant are covered in the technique **Forensics: Arson (p. 34)**.

Other

Other types of trace evidence include:

- Human and animal hair. Hair can fall from a body at any time. Hair can reveal various information about its owner, including, in some cases, their **DNA (p. 42)**. See Handbook of Trace Evidence Analysis,[35] chapter "Forensic Hair Microscopy" for an overview of hair.
- Paint. A painted object can leave traces of paint on a surface it touches. A trace of paint can reveal information about the object that left it. See Handbook of Trace Evidence Analysis,[35] chapter "Paints and Polymers" for an overview of paint.

Mitigations

Anonymous dress (p. 137): An adversary can use trace evidence to link clothing to an action site. To mitigate this, you can dress anonymously, and in particular dispose of the clothing after the action.

[71] https://en.wikipedia.org/wiki/Refractive_index
[72] https://en.wikipedia.org/wiki/Chemical_element

Anonymous purchases (p. 139): An adversary can use trace evidence to link objects to an action site. To mitigate this, you can anonymously purchase objects used in the action.

Careful action planning (p. 149): An adversary can use trace evidence to link objects to an action site. To mitigate this, after the action, you can plan to:

- Dispose of the objects you used during the action.
- If an object is too expensive to discard after each action, store it in a **stash spot or safe house (p. 174)**.
- If a tool is too expensive to discard after each action, modify it so that an adversary cannot link it to traces it may have left at the action site. For example, you can dispose of the disc of a disc cutter.

Stash spot or safe house (p. 174): An adversary can use trace evidence to link objects to an action site. To mitigate this, after the action, you can store in a stash spot or safe house objects used in the action that are too expensive to discard after each action.

Repressive operations

Case against Jeff Luers (p. 211): In the raid of the storage unit, the police found a bolt cutter matching the cuts in the fence surrounding the site of the May arson attempt.[73]

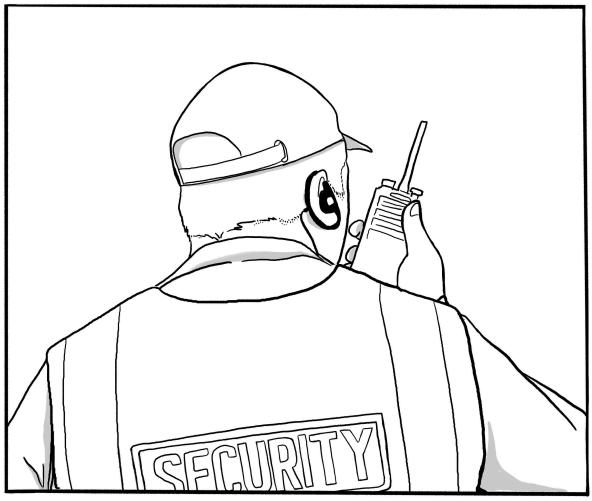
Case against Ruslan Siddiqi (p. 184): Investigators found bicycle tire marks near the train bombing site.[54] This supported the theory that the person who carried out the bombing traveled by bike.

December 8 case (p. 193): During the raids, several objects (a stove, pans, gloves, spatulas) were analyzed for traces of products that could be used to create explosives.[8]

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

3.10. Guards

Used in tactic: **Arrest**



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

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

Mitigations

Attack (p. 143): Before or during an action, you can incapacitate guards to prevent them from interfering with the action. For example, in their actions on logging companies machinery in so-called Chile, Mapuche people have neutralized guards by disarming them,[74] tying them up[75] or shooting at them.[76]

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

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

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

Reconnaissance (p. 173): Before an action, you can identify the presence of guards at the action site.

Repressive operations

Case against Louna (p. 182): In the days preceding the arson, a security guard saw suspicious vehicles driving near the arson site, took photos of them, and, after the arson, provided the photos to investigators.[7]

3.11. House raid

Used in tactics: **Arrest**, **Incrimination**

A house raid is a surprise visit of a residence conducted by an adversary to seize items, arrest occupants of the residence, or install covert surveillance devices.

When

An adversary can conduct a house raid:

- Most often, early in the morning when the occupants of the residence are asleep and taken by surprise.
- In some cases, during the day. This can be the case when one goal of the raid is to seize digital devices while they are turned on (and therefore their **encryption (p. 161)** is not effective). In this case, the adversary can decide to conduct the house raid during the day because digital devices are more likely to be turned on when their users are awake, which is more likely to be during the day.

Why

An adversary can conduct a house raid to:

- Seize items to find evidence or to do **network mapping (p. 95)**. Commonly seized items include electronic devices, literature, materials that could be used in actions, and clothing. In some cases, the adversary seizes expensive items (e.g., computers, printing equipment) with the goal of disrupting the organizational capacity of their targets.

- Arrest the occupants of the residence.
- Install **covert surveillance devices (p. 16)** in the residence.

Additional considerations

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

Mitigations

Clandestinity (p. 150): If you enter clandestinity, an adversary cannot know where you live, and therefore cannot raid your home.

Preparing for house raids (p. 171): You can prepare for a house raid by minimizing the presence of materials that could be harmful in the event of a raid.

Preparing for repression (p. 172): You can prepare for repression to minimize the impact of house raids.

Stash spot or safe house (p. 174): You can keep action materials that have no "legitimate" purpose in a stash spot or safe house, or at worst, let them pass through your home only for a very limited time.

Repressive operations

Scripta Manent (p. 210): One person was arrested after batteries and an electrician's manual were found in his home during a raid.[77]

Renata (p. 200): During a house raid, cops tried to get into the basement without waking up the people in the house, then privately complained that they were unable to hide what they wanted to hide.[78]

Case against Revolutionära fronten (p. 204): During raids on the homes of some of the defendants, investigators found:[7]

- A computer containing incriminating messages sent and received on the messaging application MSN Messenger.

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

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

- Molotov cocktails.

Repression of Lafarge factory sabotage (p. 185): Among the initial house raids, one was particularly thorough: cops searched under mattresses, behind sofa covers and in every drawer of every piece of furniture, inspected every book, notebook and piece of clothing as well as the dishes, and emptied packages of pasta and sealed jars.[79]

2013 case against Mónica and Francisco (p. 204): During a raid on the home of Mónica and Francisco, investigators found:[59]

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

Case against Louna (p. 182): Investigators raided:

- The home of the owner of the car that brought Louna to the hospital.[7] They seized the car during the raid.
- The home of a person suspected of being seen on the CCTV footage from the hospital carrying a watering jug, in the hope of finding the watering jug during the raid and confirming that the person was indeed at the hospital.[80]

Case against Jeff Luers (p. 211): During the raid of the storage unit, investigators found:[73]

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

Bure criminal association case (p. 196): During the raids, investigators found:[7]

---

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

[80]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

- Various items consistent with items used in demonstrations: containers filled with gasoline or other substances, fireworks, Molotov cocktails, and a large number of helmets.
- A backpack containing both a written document with a person's name and materials that could be used to build incendiary or explosive devices.
- An unencrypted computer containing both a person's resume and a document describing what happened during the June 21, 2017 demonstration.
- Numerous reports of sensitive meetings containing people's names or pseudonyms, both on paper and on unencrypted storage devices.

Operation 8 (p. 209): During the raids, investigators seized:[81]

- Electronic devices.
- Photos.
- Clothing items and camping gear, including tents, hiking boots, and tarps. The items were seized in an attempt to match them to similar items visible in footage of the "training camps."[6]
- Vehicles.
- Nine firearms.

Some of the raids were particularly thorough: cops searched freezers, garbage bins, and compost bins.

Repression of the attack on Clarín's headquarters (p. 187): During raids, investigators found eight national identity cards and a debit card in the names of third parties.[60] In court, the cards were presented as evidence of the defendants' "strategy of concealment" and were used to justify keeping them in preventive detention.

Case against Direct Action (p. 212): In a raid on the house where four members of Direct Action lived, investigators found:[82]

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

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

- Related to the electrical substation bombing: plans of the action site, a copy of the action claim sent after the bombing, and newspaper clippings of articles about the bombing.
- Related to the Litton Industries bombing: photographs and plans of the action site, newspaper clippings of articles about the bombing, and a pocket knife taken by a member of Direct Action from the stolen van used in the bombing.

December 8 case (p. 193): During the raids, investigators found firearms and products that could be used to create explosives.[8]

3.12. ID checks

Used in tactics: **Arrest**, **Incrimination**

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

Complying with an ID check gives the State information about you, which can help them **map your network (p. 95)**, and can lead to your arrest if you are wanted by them. The consequences of being unable or refusing to comply with an ID check are highly context-dependent, but may include having your biometric information taken by force or without your knowledge, being detained, and being deported out of the country.

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

Mitigations

Avoiding self-incrimination (p. 144): If possible, you can avoid answering questions or providing biometric information (face photograph, fingerprints, DNA) during an ID check.

Fake ID (p. 162): During an ID check, if providing your real identity could lead to your arrest or other negative consequences, you can present a fake ID (as long as the fake ID is not recognized as such by the State).

Repressive operations

Case against Boris (p. 188): Investigators obtained and analyzed records of ID checks made by local police shortly before and after the sabotages, in different perimeters around where the sabotages took place, presumably hoping to find the names of the saboteurs in those records.[22]

3.13. Increased police presence

Used in tactics: **Arrest**, **Deterrence**

Increased police presence is the process by which the police increase their presence in a particular place and time for two reasons: to intimidate, and to improve their options for intervention and their responsiveness.

Examples of increased police presence include:

- More frequent **police patrols (p. 111)** in a particular area.
- The deployment of police officers and vehicles at a public demonstration. In the hours before a demonstration begins, police officers and vehicles can cluster on the streets around the demonstration or around its expected targets. This clustering can be an opportunity for them to conduct **overt surveillance (p. 108)** before, during, and after the demonstration.

Mitigations

Attack (p. 143): If you expect the police to increase their presence at a public demonstration, you can organize to make sure the crowd is large and fierce enough: decentralized and autonomous forces are more agile than the rigid chain of command that police agencies rely on for crowd control.

For example, despite years of planning to militarize Hamburg, Germany, for the G20 summit, rioters were able to liberate a neighborhood from police occupation for an entire night.[83]

Careful action planning (p. 149): You can carefully plan an action to mitigate the risk of an increased police presence at the action site. For example:

- You can conduct a thorough **reconnaissance (p. 173)** of the action site and prepare a good escape plan.
- If you are planning to carry out arson, you can use an incendiary device with a delay so that the device is not activated until after you have left the action site.
- You can take advantage of the fact that an increased police presence in one place means the possibility of a decreased police presence elsewhere.

3.14. Infiltrators

Used in tactic: **Incrimination**

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

Stop Hunting Sheep[84] describes five basic types of infiltrators:

1. Hang Around: Less active, attends meetings, events, collects documents, observes and listens.
2. Sleeper: Low-key at first, more active later.
3. Novice: Low political analysis, "helper", builds trust and credibility over longer term.

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

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

4. Super Activist: Out of nowhere, now everywhere. Joins multiple groups or committees, organizer.
5. Ultra-Militant: Advocates militant actions and conflict.

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

See the "Infiltrators and informants" topic.[85]

Mitigations

Attack (p. 143): You can attack infiltrators when uncovered or years later[86] to discourage the practice—police infiltrators are likely to be less enthusiastic if there is a local precedent of violence against them.

Background checks (p. 146): You can perform background checks to help ensure that someone in your network is not an infiltrator.

Need-to-know principle (p. 167): You can apply the need-to-know principle to limit the information a potential infiltrator can obtain about your involvement in actions (if an infiltrator isn't involved in an action, they shouldn't know who is involved even if it's their own roommate).

Network map exercise (p. 168): You can conduct a network map exercise to make your network more resilient to infiltration attempts.

Repressive operations

Fenix (p. 203): Two police officers infiltrated the network of the defendants for several months.[87] During their infiltration, the two officers:

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

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

[87] https://antifenix.noblogs.org/post/2015/07/01/the-czech-undercover-police-agents-reveald

- Tried to convince people to carry out more "radical" actions, presumably to push people into committing crimes for which they could later be charged.
- Actively provided material support to the network (e.g., printing posters, providing transportation and paying for gasoline), presumably to be seen in a good light by people.

3.15. Informants

Used in tactic: **Incrimination**

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

An adversary can use different strategies to recruit an informant:

- Target people who are seen as more likely to become informants: people on the periphery of a network who are less committed, people who are no longer in a group or network and harbor feelings of resentment…
- Threaten someone with negative consequences if they don't become an informant: a longer prison sentence, deportation…
- Offer someone positive consequences if they become an informant: immunity or leniency in the judicial case in which they are asked to become an informant or in another case, money…

An adversary can use an informant to gather evidence or to **map a network (p. 95)**.

See the "Infiltrators and informants" topic.[85]

Mitigations

Attack (p. 143): You can attack informants when uncovered or years later to discourage others from becoming informants.

Background checks (p. 146): You can perform background checks to help ensure that someone in your network is not an informant.

Need-to-know principle (p. 167): You can apply the need-to-know principle to limit the information a potential informant can obtain about

your involvement in actions (if an informant isn't involved in an action, they shouldn't know who is involved even if it's their own roommate).

Network map exercise (p. 168): You can conduct a network map exercise to help ensure your network does not place trust in people who could be or become informants.

Prisoner support (p. 173): You can support prisoners from your networks: beyond the ethical imperative of this support, people are less likely to turn informant if they feel supported and connected to the movements for which they risked their freedom.

Repressive operations

Case against Marius Mason (p. 212): The main evidence against Marius Mason was provided to investigators by his former husband, Frank Ambrose, who had participated in some of the actions with him.[88] Frank Ambrose became an informant after his arrest in 2007 (which was triggered by him throwing incriminating material in a garbage can).[89] For several months, the snitch collaborated extensively with the Federal Bureau of Investigation (FBI), secretly recording 178 phone conversations and face-to-face meetings, and providing information on 15 people.[90]

2011-2013 case against Jeremy Hammond (p. 205): In June 2011, investigators recruited an associate of Jeremy Hammond, Sabu, as an informant.[91] For several months, Sabu helped investigators build a case against Jeremy Hammond. In exchange for their collaboration Sabu received a lenient sentence: after having spent 7 months in prison (for a bail violation), they were sentenced to time served.[92]

Sabu knew Jeremy Hammond's online persona but did not know his real life identity. To find out Jeremy Hammond's real life identity, investigators

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

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

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

[91] https://rollingstone.com/culture/culture-news/the-rise-and-fall-of-jeremy-hammond-enemy-of-the-state-183599

[92] https://latimes.com/nation/nationnow/la-na-nn-hacker-sabu-sentenced-20140527-story.html

used information that he had shared with Sabu in online chats, including that:[93]

- He had been arrested at the 2004 Republican National Convention, had spent time in a federal prison and in a county jail, and was currently on probation. Investigators were able to verify all of this using police files.
- Comrades of his had been arrested at a specific protest. Investigators were able to verify that an "associate" of Jeremy Hammond had attended the protest.
- He practiced dumpster-diving. Investigators saw him getting food from dumpsters during a physical surveillance operation.

Operation 8 (p. 209): At least two informants were active as part of the operation.[94] In particular:

- Informants provided investigators with background information on the defendants and the dates of the "training camps."
- An informant offered to sell someone a shotgun, presumably so that person could later be charged with possessing the shotgun.

3.16. International cooperation

Used in tactics: **Arrest**, **Incrimination**

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

International cooperation can be used to:

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

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

[93]https://notrace.how/documentation/jeremy-hammond-affidavit.pdf
[94]https://putatara.net/2015/10/05/informants

Repression against Zündlumpen (p. 191): House raids were conducted Austria, targeting people suspected of being close to N. and M.[9]

Bialystok (p. 195): In June 2020, people were arrested in Spain and France, thanks to cooperation between Italian, Spanish and French intelligence and police forces.[95]

During the investigation Italian cops tried to target a person living in Germany.[96] They sent several requests to German police to extradite the person or have their house searched but the requests were rejected.

Scintilla (p. 201): Carla was arrested in France thanks to cooperation between Italian and French intelligence and police forces.[97]

Bure criminal association case (p. 196): Some of the people that were arrested had participated in demonstrations against the 2017 G20 summit in Hamburg, Germany.[7] Because of this, German investigators cooperated with French investigators, including by being present when the people were interrogated after their arrest.

3.17. Interrogation techniques

Used in tactic: **Incrimination**

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

Interrogation techniques can include lying, making threats, instilling guilt, shame, or pride, trying to appear friendly and helpful or, on the contrary, threatening and violent, etc. In some cases, they can include **physical violence (p. 108)**.

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

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

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

See How the police interrogate and how to defend against it[98] (in French and German) for a comprehensive overview of police interrogation techniques.

Mitigations

Avoiding self-incrimination (p. 144): You should not talk to an adversary under any circumstances: this is the best way to resist their interrogation techniques.

Repressive operations

Case against Boris (p. 188): When interrogating people close to Boris, investigators used elaborate lies to try to get information from them.[22] For example, the investigators vaguely suspected that the people being interrogated had hosted Boris in April 2020 and wanted to confirm their suspicion, so they asked, "Our investigation revealed that you let [Boris] stay with you in April 2020. How long did he stay with you?"

Warsaw 3 (p. 201): A few weeks into his detention, one person gave an "extensive" testimony to the police. He claimed this was partly because of two techniques used by one of his lawyers to push him to give this testimony:[99]

- The lawyer showed him a social media post written by someone from his political scene shortly after his arrest. The post criticized the action for which he had been arrested and did not include a declaration of solidarity. Because the post was the only reaction from his political scene that the person knew about, he felt isolated.
- The lawyer told him that the two other people had already given extensive testimonies to the police, which was a lie.

Case against Ruslan Siddiqi (p. 184): After his arrest, investigators were unsure of Ruslan Siddiqi's involvement in the train bombing.[100] They interrogated him and deduced that he was hiding something. Ruslan

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

[99] https://wawa3.noblogs.org/post/2017/05/24/olsen-gang-replies-statements-of-warsaw-three-en

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

Siddiqi recounts: "They started asking various questions about what I was doing on [the day of the bombing]. I made a couple of blunders in my answers, and [the person in civilian clothes] who asked the questions realized that I was hiding something."

December 8 case (p. 193): When interrogating defendants during custody, investigators:[8]

- Pretended that the defendants would not be charged if they snitched on the other defendants, which was a lie.
- Threatened one of the defendants with sexual assault.

3.18. Mass surveillance

Used in tactics: **Deterrence**, **Incrimination**

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

3.18.1. Civilian snitches

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

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

Mitigations

Anonymous dress (p. 137): You can dress anonymously to prevent civilians from providing a description of you that would be valuable to an adversary.

Attack (p. 143): If a civilian follows you after an action, you can scare them off with threats or pepper spray. If a civilian tries to call the police, you can destroy their phone.

Careful action planning (p. 149): Civilians can observe you during an action and report their observations to an adversary. To mitigate this,

you can carry out actions at night or in areas with minimal foot traffic to minimize witnesses, and use a lookout to report the presence of any witnesses as soon as they are noticed. Beware of balconies and windows overlooking the action site.

Repressive operations

Fenix (p. 203): When Lukáš Borl was in clandestinity his photo and personal information were published on the national police website to encourage civilians to send information about him to the police.[101]

2019-2020 case against Mónica and Francisco (p. 190): The saleswoman of the cell phone store where Mónica bought a phone that was used as part of the 2020 action, when questioned by investigators, gave a description of a person that the investigators matched to Mónica.[45]

Arrest of Stecco (p. 194): After arresting Stecco, investigators showed his picture and asked questions to many people living around the arrest site, which allowed them to find the house where Stecco allegedly lived.[17]

Case against Amos Mbedzi (p. 207): When the explosive device exploded prematurely and severely wounded Mbedzi, a civilian was traveling by car on a nearby road.[52] The civilian stopped near the bombing site, saw another car stop, and saw Mbedzi shout "Hospital! Hospital!" and get into the other car. The civilian stayed at the site and informed the first cops who arrived that a man wounded in the explosion had gotten into a car towards a hospital. This seemingly led to Mbedzi's arrest at the hospital one hour later.

Additionally, three civilians provided investigators with visual descriptions of Mbedzi: the aforementioned civilian, the driver of the car that took Mbedzi to the hospital, and the hospital security guard. This helped investigators reconstruct Mbedzi's movements and prove that he was at the bombing site.

Case against Louna (p. 182): Several civilians helped investigators. In particular:[7]

[101] https://antifenix.noblogs.org/post/2016/03/11/confirmed-lukas-borl-under-police-investigation

- After hearing Louna make an appointment with a doctor through an intercepted phone call, investigators contacted the doctor, who provided them with Louna's personal information, including her address and phone number.
- The pharmacist at a pharmacy where Louna obtained medication provided a physical description of Louna, confirmed recognizing her from a photograph, and provided personal documents of hers, including copies of prescriptions.
- The director of a higher education institution where a person studied provided the person's class schedule and information about the transportation they used to get to the institution.

Belarusian anarcho-partisans (p. 188): While trying to cross the Belarusian-Ukrainian border, the people stopped at a shop about 10 kilometers from the border.[7] A shopkeeper called the border guards on them, which led directly to their arrest.

Case against Ruslan Siddiqi (p. 184): In the weeks following the train bombing, investigators interrogated many citizens in a large area surrounding the bombing site.[54]

In particular, investigators interrogated a shop clerk in a village. The clerk told investigators that, before the bombing, someone wearing a camouflage jacket and carrying a backpack had passed by the shop. The clerk provided a description of the person, which investigators used to create a composite sketch. Three weeks after the bombing, Ruslan Siddiqi encountered a local cop who compared him with the composite sketch and arrested him.

Case against Direct Action (p. 212): Several civilians helped investigators.[11] In particular:

- Journalists told investigators that they had noticed similarities between action claims published by Direct Action and articles in a local quarterly publication called Resistance.
- A hunter, presumably by chance, discovered two wooden structures where members of Direct Action stored the stolen explosives they used in bombings, and alerted the police to the discovery.[82]

- The landlords of the house where four members of Direct Action lived gave investigators the key to the house so they could enter and install hidden microphones.

3.18.2. Mass digital surveillance

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

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

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

See the "Digital surveillance" topic.[102]

Mitigations

Avoiding self-incrimination (p. 144): An adversary can use mass digital surveillance to retrieve self-incriminating information from a digital device. To mitigate this, you can avoid storing such information on digital devices

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

except for very deliberate reasons (such as writing and sending an action claim while following **digital best practices (p. 152)**).

Digital best practices (p. 152): You can follow digital best practices to make mass digital surveillance ineffective. For example, you can use Tor[103] to anonymize your Internet activity, and you can use security-oriented operating systems and applications that limit the data they store or collect about you.

Encryption (p. 161): You can encrypt "in-motion" data to prevent observers at certain points on the network from analyzing this data.

3.18.3. Police files

Police files are physical or digital records maintained by law enforcement agencies. Police files contain vast amounts of data about many things, are kept indefinitely or for long periods of time, and can be efficiently analyzed and cross-referenced using digital tools.

Notable examples of police files include:

- Databases of government-issued ID documents (ID cards, driving licenses, passports).
- Databases of biometric information (face photographs, fingerprints, DNA).
- Records of **ID checks (p. 76)**, fines, arrests, investigation proceedings, judicial proceedings, and convictions.

Mitigations

Attack (p. 143): You can destroy cabinets that store police files on paper and data centers that store them digitally.

Repressive operations

Case against Boris (p. 188): Investigators found out that the DNA on the bottle cap belonged to Boris because his DNA was in France's national DNA database.[22]

[103] https://torproject.org

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

2011-2013 case against Jeremy Hammond (p. 205): Under his online persona, Jeremy Hammond shared in online chats that he had been arrested at the 2004 Republican National Convention, had spent time in a federal prison and in a county jail, and was currently on probation.[93] Investigators were able to verify all of this using police files, which helped them to link Jeremy Hammond's online persona to his real life identity.

Bure criminal association case (p. 196): Investigators extensively used police files to establish links between people, including databases of driver's licenses and registered vehicles, as well as records of arrests, judicial proceedings and convictions.[7]

3.18.4. Video surveillance

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

Collection

Sources of CCTV footage include:

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

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

Storage

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

Analysis

An adversary can analyze CCTV footage:

- In real time if the cameras are integrated into a central network. Real-time analysis can take place either as part of routine surveillance or during exceptional events (e.g. demonstrations).
- Retroactively if the CCTV footage has been stored. Retroactive analysis can help identify a suspect by their **face (p. 52)**, **gait (p. 55)**, **voice (p. 62)**, etc.

Analysis of CCTV footage can be performed:

- By humans.
- By automated systems such as automated license plate readers or **facial recognition systems (p. 52)**.

See also

- You Can't Catch What You Can't See: Against Video Surveillance.[104]
- The topics "Video surveillance"[105] and "Automated license plate readers".[106]

Mitigations

Anonymous dress (p. 137): You can dress anonymously to prevent an adversary from identifying you from CCTV footage.

Anonymous purchases (p. 139): You can make anonymous purchases to prevent an adversary from identifying you from CCTV footage of physical stores.

[104] https://notrace.how/resources/#catch-see

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

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

Attack (p. 143): You can disable[107] surveillance cameras.

Biometric concealment (p. 147): When filmed by surveillance cameras, you can:

- To prevent **gait recognition (p. 55)**, wear baggy clothing that hide your body shape, use an umbrella or other concealing objects, or drastically change your walking style by adopting a "funny walk".
- To prevent **facial recognition (p. 52)**, wear a mask to cover your facial features, and sunglasses or a hat with a low brim to cover your eyes.

Outdoor and device-free conversations (p. 169): You can conduct sensitive conversations away from surveillance cameras to prevent an adversary from recording those conversations with surveillance cameras equipped with microphones.

Reconnaissance (p. 173): Before an action, you can identify the location of surveillance cameras at an action site and make plans to avoid them if possible.

Transportation by bike (p. 180): You can use a bike instead of any other type of vehicle: compared to other vehicles, a bike is much harder to identify on CCTV footage, especially if its distinguishing features are minimized. For example, you can use a different stolen bike for each action you carry out.

Repressive operations

Case against Boris (p. 188): Soon after the April sabotage, investigators requested CCTV footage from businesses and municipal cameras, and lists of vehicles from automated license plate readers (ALPRs) and speed cameras, all within an extended perimeter of the sabotage site.[22]

2019-2020 case against Mónica and Francisco (p. 190): Public CCTV footage was extensively used by investigators to reconstruct the movements of Mónica and Francisco before and during the actions, despite the mitigations they took (taking taxis, changing clothes, wearing disguises).[45]

Repression against Zündlumpen (p. 191): Three weeks before an arson, a wildlife camera near the arson site captured a person walking, wearing an

[107] https://notrace.how/resources/#destroy-cameras

orange jacket.[9] After the arson, investigators obtained the camera footage and claimed that the jacket resembled one that M. had worn at some point.

Case against Revolutionära fronten (p. 204): CCTV footage from cameras near the scene of the Stockholm beating showed that some of the defendants were present during the beating.[7]

Repression of Lafarge factory sabotage (p. 185): Immediately after the action, investigators requested CCTV footage from public transportation (buses, train stations, etc.), businesses, home surveillance systems, and municipal cameras, all within an extended perimeter of the action site.[50] In particular, footage of the interiors of buses appears to have helped identify people traveling to and from the action site.[49] Investigators also requested footage from highway toll booths, presumably to identify the occupants of known cars traveling on highways to or from the action site.

Prometeo (p. 199): Two of the people were allegedly seen on video surveillance leaving a store where investigators believe the envelopes used to prepare the parcel bombs were purchased.[30]

Arrest of Stecco (p. 194): Investigators analyzed CCTV footage from street cameras, train stations, highway toll booths, buses, and businesses to determine the movements of people under surveillance.[17]

2013 case against Mónica and Francisco (p. 204): Public CCTV footage was used by investigators to reconstruct the movements of Mónica and Francisco before and after the action.[59] This showed that they were near the action site shortly before the explosion of the device.

Case against Peppy and Krystal (p. 183): CCTV footage from a bus allowed investigators to identify the license plate of the motorcycle on which Peppy and Krystal arrived at and left the protest site.[10]

Case against Louna (p. 182): CCTV footage from the arson site showed two people setting fire to the excavator, and one of them burning themselves accidentally.[80]

CCTV footage from the hospital on the night of the arson showed:

- The license plate of the car that brought Louna to the hospital.
- The faces of the other people in the car.

- One of the people in the car carrying a watering jug. Investigators would later try to find this watering jug during a house raid.

CCTV footage from cameras in several towns was used to try to reconstruct the route of the car that brought Louna to the hospital, and the route Louna took when she left the hospital.[7]

Repression of the first Jane's Revenge arson (p. 185): CCTV footage helped identify a vehicle driven by the person, when they were seen entering a parking lot on foot after a demonstration, and the vehicle was seen leaving the same parking lot a few minutes later.[39]

Bure criminal association case (p. 196): Investigators used footage from the demonstrations, recorded by surveillance cameras and police forces, to:[7]

- Identify a person who was only partially masked, with their eyes, glasses, and forehead visible.
- Match a person who looked pregnant based on their belly, seen in a demonstration, to a person who gave birth a few months later.

The three from the park bench (p. 192): On the evening leading up to the arrest, one of the people—while being followed by cops—stopped at a gas station and was seen by the station's video surveillance cameras buying gas and filling a gas can.[108] The cops obtained the CCTV footage the next morning.

Case against Ruslan Siddiqi (p. 184): CCTV footage from factories near the train bombing site showed someone riding a bike shortly before and after the bombing, wearing camouflage clothing and carrying a backpack.[54] This supported the theory that the person who carried out the bombing traveled by bike.

Repression of the attack on Clarín's headquarters (p. 187): CCTV footage from multiple cameras showed one defendant leaving the attack site, being driven away on a motorcycle for a few blocks, and boarding a bus—the defendant was identified because he used his partner's electronic bus card to board the bus.[109]

---

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

[109] https://web.archive.org/web/20211210123411/https://www.revolucionpopular.com/otras-noticias/la-policia-detuvo-a-otro-hombre-por-el-ataque-a-clarin_a61b34174d2f0a04884749d24

3.19. Network mapping

Used in tactic: **Incrimination**

Network mapping is the process by which an adversary gains insight into the organization and social relationships of a given network. By gaining this insight, an adversary can select individuals for additional scrutiny, arrest, or recruitment as **informants (p. 80)**.

The State very frequently uses social media friends lists (a form of **open-source intelligence (p. 97)**) for network mapping because they do not require a warrant or legal authorization.

Mitigations

Anonymous phones (p. 138): You can use anonymous phones to make it harder for an adversary to map your network.

Avoiding self-incrimination (p. 144): An adversary can use information obtained through self-incrimination to endanger not only the individual from whom the information was obtained, but also the rest of their network. To mitigate this, you should not talk to an adversary under any circumstances, and you can avoid providing biometric information (face photograph, fingerprints, DNA) if possible.

Compartmentalization (p. 151): You can compartmentalize your different identities (or projects) to make it harder for an adversary to map your network.

Digital best practices (p. 152): You can follow digital best practices, and in particular use end-to-end encrypted messaging applications on encrypted devices, to obscure your social networks and make it harder for an adversary to map your network.

Fake ID (p. 162): During an ID check, you can present a fake ID to make it harder for the State to map your network.

Need-to-know principle (p. 167): You can apply the need-to-know principle to make it harder for an adversary to map your network.

Network map exercise (p. 168): An adversary can map a network by using infiltrators and informants to monitor the network: infiltrators and

informants build credentials through association, build social profiles of people in the network, find pressure points to instigate interpersonal and political conflict, and entrap people. To mitigate this, you can conduct a network map exercise to make your network more resilient to infiltration attempts and help ensure it does not place trust in people who could be or become informants.

Repressive operations

Repression against Zündlumpen (p. 191): Investigators claimed that because N. and M. were partners, they likely committed arson together.[9]

Mauvaises intentions (p. 208): To prove that the defendants knew each other and were therefore likely accomplices, the investigators used several clues:[37]

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

Operation 8 (p. 209): Before the raids, investigators spent several months establishing links between people by examining metadata from:[6]

- Phone calls (both mobile and landline).
- Phone text messages.
- Emails.

Repression of the attack on Clarín's headquarters (p. 187): After identifying the first defendant, investigators identified the other defendants by establishing links between them. Investigators found that the defendants:[60]

- Called each other on the phone.
- Were part of the same groups on the messaging application WhatsApp.
- Interacted with each other on the social network Facebook.

3.20. Open-source intelligence

Used in tactic: **Incrimination**

Open-source intelligence (OSINT) is the collection and analysis of data from open sources (social media, news media, blogs, forums, public records…)

Mitigations

Avoiding self-incrimination (p. 144): An adversary can use open-source intelligence to collect information that you publish voluntarily. To mitigate this, you can avoid using social media and generally avoid making any information about yourself or your networks public.

Repressive operations

2019-2020 case against Mónica and Francisco (p. 190): The photos used to identify Mónica and Francisco in public CCTV footage were found on social media.[45]

Repression against Zündlumpen (p. 191): Investigators:[9]

- Analyzed several anarchist publications and websites, including two that they considered to be "successor projects" to Zündlumpen.
- Suspected N. of contributing to a French-language anarchist website because she spoke French fluently.

Search for a fugitive (p. 189): Investigators analyzed the posts made by the person on the social media Instagram from 2019 to 2022 and found:[7]

- A post that included the personal information of United States Immigration and Customs Enforcement (ICE) agents.
- A mention of the person working for a company, which led investigators to request information about the person from that company.

Case against Revolutionära fronten (p. 204): A video of the Stockholm beating, which was filmed and posted online by the Revolutionära fronten, showed that some of the defendants were present during the beating, even

though their faces were blurred[110] in the video.[7]

Repression of Lafarge factory sabotage (p. 185): Investigators collected metadata from photos of the action posted online, including the name and serial number of a camera.[50] This helped them identify a person they accused of taking the photos.

Bure criminal association case (p. 196): Investigators visited a Facebook page associated with the struggle against Cigéo and then analyzed the Facebook profiles of everyone who had "liked" the page.[7]

Operation 8 (p. 209): Investigators obtained information on people from web searches and newspaper articles.[6]

Repression of the attack on Clarín's headquarters (p. 187): Investigators analyzed social media profiles to establish links between the defendants.[60] The profile of one defendant on the social network Facebook was named "Coctel Molotov" (*Molotov cocktail*), which was considered suspicious.

3.21. Parallel construction

Used in tactic: **Incrimination**

Parallel construction is the unlawful law enforcement process of building a parallel, or separate, evidentiary basis for an investigation in order to conceal how an investigation was actually conducted.

For example, an intelligence agency can collect incriminating digital evidence from a phone without a warrant, and then conduct a **house raid (p. 72)** to seize the phone where that evidence can be "discovered" so that it will not be thrown out at trial because it was obtained illegally.

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

[110] https://aftonbladet.se/nyheter/a/WL8EEd/atal-mot-vansterextremister-i-revolutionara-fronten

3.22. Physical surveillance

Used in tactic: **Incrimination**

Physical surveillance is the direct observation of people or activities for the purpose of gathering information. A *physical surveillance operation* is typically conducted by one or more *surveillance teams*, which consist of specially trained personnel called *surveillance operators*.

Because it requires the deployment of surveillance operators on the ground, sometimes for extended periods of time, physical surveillance is usually a resource-intensive and personnel-intensive method of surveillance.

3.22.1. Aerial

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

Examples of aerial physical surveillance include:

- Observing the crowd during demonstrations or gatherings, often as part of an **overt (p. 108)** surveillance operation.
- Improving the chances of successfully following the target of surveillance during a **covert (p. 101)** surveillance operation, especially at night.
- Locating suspects soon after an action took place and the adversary has been alerted, especially in rural areas or at night (in the case of an arson in Germany, a police helicopter responded by flying over the area the same night[111]).
- Locating suspects as part of routine **police patrols (p. 111)** in areas at risk of criminal activity.

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

Surveillance planes can monitor entire cities, photographing up to 80 square kilometers per second, allowing for the slow-motion reconstruction of virtually any outdoor movement,[112] with high-quality video at night.[113]

See the "Aerial surveillance" topic.[114]

Mitigations

Anonymous dress (p. 137): If you are being followed by an aerial surveillance operation, you can change into anonymous clothing when you are in a location that is not visible from the air to make it harder for the aerial surveillance operation to re-establish contact with you when you emerge into an open area (this won't work if the surveillance operation is also observing you on the ground).

Anti-surveillance (p. 141): You can include in an anti-surveillance route locations that would prevent an aerial surveillance operation from following you: an underground metro system, a shopping complex with many entrances, etc.

Attack (p. 143): During a demonstration, you can take down drones with fireworks, hack them, or blind them with lasers. See also 5 widely accessible ways to take down drones.[115]

Surveillance detection (p. 176): You can conduct surveillance detection to detect most and helicopters and some drones by listening for potential helicopters and drones: you should be able to hear most of them, depending on their altitude and your surroundings.

Repressive operations

Repression against Zündlumpen (p. 191): Drones were used to follow N. and M. in a forest during a covert physical surveillance operation.[9]

Berlin 2023 railway conspiracy case (p. 183): The arrested people were discovered at night by a helicopter on a routine surveillance flight,

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

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

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

[115] https://notrace.how/resources/#5-ways

presumably equipped with night-vision equipment.[116] A text[117] reports that in 2022, during another routine surveillance flight near Berlin, the same helicopter turned off its position lights and muffled the sound of its rotor blades to avoid detection: "Although the helicopter could still be heard, the noise was diminished. This can lead to misjudging the distance of the helicopter or, if mixed with other noise such as a highway, not being aware of the approaching problem until it's too late."

Operation 8 (p. 209): On the morning of the October 15 raids, a police helicopter was flying over an area where several raids were taking place, seemingly to surveil the area.[81]

Repression of the 2019 uprising in Chile (p. 192): Drones were used to track rioters leaving riots in order to facilitate their arrest.[118]

Case against Direct Action (p. 212): After investigators discovered the remote area where members of Direct Action hid the stolen explosives they used in bombings, they arranged for a helicopter to fly over the area daily for surveillance purposes.[11]

3.22.2. Covert

Covert physical surveillance is the direct observation of people or activities when the surveillance operators do not want to be detected by their targets.

Mobile

A mobile physical surveillance operation is typically conducted by a surveillance team of five to twenty operators using multiple vehicles, and typically begins with a static phase: staking out the location where the target is believed to be, such as their home or place of employment. When the target leaves the stakeout location, the surveillance team begins following them and the surveillance operation transitions into a mobile phase. The

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

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

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

surveillance operation then alternates between static phases (when the target stops) and mobile phases (when the target starts moving again).

Examples of mobile physical surveillance techniques include:

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

Mobile physical surveillance may be facilitated by:

- A **tracking device (p. 21)** installed on the target's vehicle or bike.
- Real-time geolocation of the target's phone, obtained with the **collaboration of mobile network operators (p. 114)**.
- **Aerial surveillance (p. 99)**, such as a drone following the target from a distance.

Static

Static physical surveillance is the observation of a target when the target cannot move, or the surveillance operators do not intend to follow them if they move. A static physical surveillance operation is typically conducted by a surveillance team using one or more vehicles.

An example of a static physical surveillance operation is parking a surveillance vehicle in front of a target's home, with surveillance operators inside the vehicle watching the entrance to the home.

Arrest

Generally, a surveillance team will not attempt to arrest its target during a covert physical surveillance operation. On rare occasions, however, this may happen if the surveillance team has gathered enough information

about the target's activities to incriminate them and deems it necessary to arrest the target immediately (e.g. to prevent a crime).

See also

- Surveillance Countermeasures[119] about the principles and techniques of covert physical surveillance.
- Measures Against Surveillance[120] for insights into how police and intelligence agencies conduct covert physical surveillance.
- The "Physical surveillance" topic.[121]

Mitigations

Anti-surveillance (p. 141): You can conduct anti-surveillance to evade a covert physical surveillance operation.

Surveillance detection (p. 176): You can conduct surveillance detection to detect a covert physical surveillance operation.

Transportation by bike (p. 180): You can use a bike instead of any other type of vehicle: compared to other vehicles or people on foot, a bike is harder to follow by a covert physical surveillance operation, especially without the operation being detected.

Repressive operations

Case against Boris (p. 188): For several weeks, investigators regularly staked out Boris's home and tailed him as he moved on foot, on bicycles, and in vehicles.[22]

Repression against Zündlumpen (p. 191): Investigators followed N. for 15 days.[47]

Search for a fugitive (p. 189): In 2022, a surveillance operator conducted, alone, covert physical surveillance of a residence.[7] Three days prior, investigators had obtained the address of the residence through the

[119] https://notrace.how/resources/#surveillance-countermeasures
[120] https://notrace.how/resources/#measures-surveillance
[121] https://notrace.how/resources/#topic=physical-surveillance

collaboration of the Supplemental Nutrition Assistance Program,[122] and had also obtained the list of purchases made through the program in the past three months. The operator saw someone drive out of the residence who matched the person's description, but failed to follow them because they were "traveling too fast." The operator then went to a nearby gas station convenience store that appeared frequently on the list of purchases. There, they found the person again. The operator asked a nearby city police officer to assist with arresting the person, but the officer declined, partly because they were in a "non-enforcement capacity." The operator then requested assistance from state police, but before state police could intervene, the person had left the gas station. As the person drove away, the operator attempted to grab their wrist. Fifteen minutes later, the operator drove past the residence and saw the person leaving in the passenger seat of a vehicle but failed to follow due to heavy traffic.

Arrest of Stecco (p. 194): Investigators learned through a hidden microphone installed in a home that someone under surveillance would be traveling by train the next day.[17] The next day, this person and another indeed traveled by train and a large number of surveillance operators were deployed to follow them. There were four operators on the train (two at each end) and two operators waiting at each intermediate station.

Case against Peppy and Krystal (p. 183): A week before the protest, investigators conducted covert physical surveillance at a local bookstore where they knew people planning the protest were organizing.[10] They observed Peppy enter the bookstore and leave an hour and a half later.

A few days after the protest, investigators conducted covert physical surveillance at the home of Peppy and Krystal. They observed Peppy and Krystal riding the same motorcycle they used to arrive at and leave the protest site.

2011-2013 case against Jeremy Hammond (p. 205): During a physical surveillance operation against Jeremy Hammond's home that lasted several days, investigators established a correlation between:[93]

[122] Supplemental Nutrition Assistance Program (SNAP) is a government food-purchasing assistance program. Each month, beneficiaries receive money on a special debit card that is part of an electronic system called electronic benefit transfer (EBT). Beneficiaries can use the card to purchase food.

- The times when Jeremy Hammond was physically present at his home.
- And the times when his online persona was reported as being online by the informant Sabu.

Case against Louna (p. 182): After the arson on the night of May 4 to May 5, 2024, investigators conducted several physical surveillance operations:[7]

- On May 5, at the hospital, they took photos of people asking after Louna and listened to conversations.
- On May 6, 7, 11, and 14, they surveilled places where people opposed to the highway project lived. They took photos of vehicles and noted their license plates.
- On May 10, they surveilled the entrance of the hospital, where Louna had an appointment.
- In July, they surveilled an event organized by a person opposed to the highway project.

At the beginning of October, an arrest warrant was issued for Louna. Until her arrest on October 12, 2024, investigators conducted several physical surveillance operations:

- On October 3, they:
  - Surveilled the homes of Louna's parents and grandparents for 6 hours.
  - Drove by another home of Louna's family several times in a vehicle.
  - Followed a person seen with Louna at the hospital for 4 hours.
- On October 8, they:
  - Surveilled the homes of Louna's parents and grandparents again for 6 hours.
  - Drove by the homes of several members of Louna's family and a person who had accompanied her to the hospital several times.
  - Followed a person seen with Louna at the hospital again for 6 hours.
- On October 10, during the trial of a person opposed to the highway project, they surveilled the interior of the courthouse and the surrounding area.

- On October 12, after hearing about a meeting outside apartment buildings through an intercepted phone call, they surveilled those buildings and arrested two people who went to the meeting, including Louna.

Repression of the first Jane's Revenge arson (p. 185): In March 2023, cops secretely observed the person from a distance of about 30 meters.[39] The cops watched the person discard a bag, retrieved it, and collected DNA evidence linking the person to the action site.

Case against Jeff Luers (p. 211): On the night of the June arson, the arsonists were being tailed by a surveillance team—police officers in one or more unmarked cars—as they drove to the arson site.[73] They parked their car close to the arson site, watched by the surveillance team. They got out of their car to continue on foot, at which point the surveillance team lost sight of them. They ran back to their car 10 minutes later, at which point the surveillance team regained sight of them. They drove away from the arson site. More than an hour later, the surveillance team—still tailing the arsonists—heard on the police radio system about a fire at the arson site and asked local police officers to stop the arsonists' car for a roadside check, suspecting that they were involved in the fire. Half an hour later, when fire investigators at the arson site reported that they believed the fire had been set intentionally, the arsonists were arrested.

Bure criminal association case (p. 196): Investigators:[7]

- Followed one of the people who were arrested for a few hours on one occasion, and for a few minutes on another, to find out where they lived.
- Spent several days conducting static surveillance on a place associated with the struggle against Cigéo (a few isolated buildings surrounded by fields). For up to 16 hours a day they took notes and pictures of people and vehicles entering and leaving the location.

The three from the park bench (p. 192): During the evening leading up to the arrest, two of the people rode their bikes through the city and were followed by cops on bikes (and presumably also cops in cars) until they were arrested in the park.[108] The cops decided to follow the people specifically that evening because it was exactly two years since the G20

summit in Hamburg and they were suspected of planning an action for the anniversary of the summit.

Operation 8 (p. 209): Investigators regularly followed people on foot and in vehicles.[6]

Investigators regularly conducted covert surveillance operations near the "training camps," but did not get close enough to see what was happening and could only hear shots being fired.[7]

Nea Filadelphia case (p. 207): On the day of the arrests, when one person visited a cybercafé that was probably under police surveillance, cops recognized him and started following him.[123] He then moved through the streets of Athens for a few hours, gradually joining the other people—some of whom were wanted by police[124]—and all of them were arrested.

Case against Direct Action (p. 212): For several weeks, investigators followed members of Direct Action and some of their friends as they moved on foot and in vehicles.[11]

On at least one occasion, investigators witnessed a member of Direct Action conducting **anti-surveillance (p. 141)** maneuvers, which they found suspicious.

December 8 case (p. 193): For several weeks, investigators staked out the homes of some of the defendants and tailed them when they moved.[20] In particular:

- When investigators staked out a defendant's home, they took pictures of anyone who entered or left the home. If the defendant left, they were followed either by the surveillance operators conducting the stakeout or by other operators so that the stakeout could continue. If the defendant left in a vehicle, they were followed in a vehicle.
- In one case, a defendant was followed into a store, and the surveillance operator took note of the items the defendant purchased and took a picture of them in the store.

---

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

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

3.22.3. Overt

Overt physical surveillance is the direct observation of people or activities when the surveillance operators intend to be, or do not mind being, detected by their targets. This is common practice at demonstrations and gatherings to identify participants, whether to facilitate **network mapping (p. 95)** or to incriminate individuals for actions carried out during the demonstration.

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

Mitigations

Anonymous dress (p. 137): You can dress anonymously at a demonstration or other event to make it harder for an overt surveillance operation to identify you.

Repressive operations

Mauvaises intentions (p. 208): During a demonstration, the investigators took 180 photographs from which they obtained 200 portraits of the demonstrators, including ten people they were able to identify.[37]

3.23. Physical violence

Used in tactics: **Deterrence**, **Incrimination**

Physical violence is the use of physical force by an adversary to intimidate a target or its network, incapacitate a target, or coerce a target into revealing information.

In some contexts, physical violence can include torture. For example, in Russia and Belarus, several anarchists have been tortured in recent years after being arrested by the State. Reported acts of torture in these countries

include:[125]

In some contexts, physical violence can include assassinations.

Mitigations

Need-to-know principle (p. 167): If you or members of your network are at risk of being tortured by an adversary, you can apply the need-to-know principle so that each person knows as little sensitive information as possible and therefore has as little information as possible to give to torturers.

See "Under the Enemy's Blade: A Search for Anarchist Practices Against Torture"[126] about practices against torture.

Preparing for repression (p. 172): If you or members of your network are at risk of being tortured by an adversary, you can prepare for that risk. For example, you can:

- Set up communication protocols that allow learning as quickly as possible when someone is arrested, in order to take immediate steps to:
  - Protect the arrested person. In some contexts where torture is limited to the first hours or days of detention, putting pressure on the adversary as soon as possible after the arrest (e.g. by involving lawyers or journalists) may help to stop the torture or limit the severity of the acts of torture.
  - Protect those who are still free, in case the arrested person "talks." This will depend on what the arrested person knows, and can include abandoning **safe houses (p. 174)**, discontinuing projects, entering **clandestinity (p. 150)**, etc.
- Prepare psychologically to resist torture.

See "Under the Enemy's Blade: A Search for Anarchist Practices Against Torture"[126] about practices against torture.

125

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

126 https://notrace.how/resources/#under-enemy-blade

Network (p. 198): Most of the defendants were tortured by the Russian Federal Security Service (FSB) in the early stages of their detention in order to obtain (often fabricated) statements that could later be used to charge and convict them.[127] Most of the defendants who were tortured later retracted their statements and spoke publicly about the torture they had received.

Renata (p. 200): During a house raid, one of the arrested people was forced to his knees by a cop who put a gun to his temple.[78]

Case against Amos Mbedzi (p. 207): Mbedzi was tortured in the first days of his detention.[52]

Belarusian anarcho-partisans (p. 188): The people were tortured in the first days of their detention.[128]

Warsaw 3 (p. 201): The people were tortured during their arrest and in the first hours of their detention.[99]

Case against Ruslan Siddiqi (p. 184): Ruslan Siddiqi was tortured for several days after his arrest.[100] Under torture, he confessed to carrying out the train bombing and the attack on the military airfield.

The torture included:[129]

Repression of the 2019 uprising in Chile (p. 192): In the streets and in custody, police forces and soldiers injured, sexually assaulted, raped, tortured and killed many protesters in what appeared to be a strategic attempt to deter participation in the uprising.[118]

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

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

[129] beatings and electric shocks.

3.24. Police patrols

Used in tactics: **Arrest, Deterrence, Incrimination**

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

Means of transportation

Police patrols can use different means of transportation:

- Marked or unmarked vehicles.
- Foot movement.
- **Helicopters, drones and surveillance planes (p. 99)**.

Routine patrols

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

Patrols in response to a threat

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

- A routine patrol stumbling upon the threat by chance.
- **Guards (p. 71)** or **civilians (p. 85)**.
- An **alarm system (p. 12)** (e.g. motion detectors inside a building), either directly or through a security company monitoring the alarm system.
- Police officers monitoring live **CCTV footage (p. 90)**.
- An **infiltrator (p. 78)** or an **informant (p. 80)**.

Mitigations

Attack (p. 143): The police can disturb an action. To mitigate this, you can distract them by launching a near-simultaneous attack on the other side of the neighborhood, or disrupt their communications by burning the cell tower used for police communications.

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

Careful action planning (p. 149): You can carefully plan an action to take into account the risk of routine police patrols interfering with the action, a risk that is always present, except perhaps in remote areas.

Reconnaissance (p. 173): Before an action, you can identify the nearest police station, their shift change schedule, and patrol patterns, and you can identify routes that are not visible to police patrols and that would make pursuit difficult (forests, railroad tracks, etc.)

Repressive operations

Repression against Zündlumpen (p. 191): Investigators sent a police patrol outside of N.'s apartment every night at irregular times to check if she was at her apartment.[47]

Case against Revolutionära fronten (p. 204): After the nighttime visit to the fascist's house, the fascist called the police, who sent out a patrol.[7] On its way to the house, the patrol stopped the defendants' car, presumably because it looked suspicious, and checked their identities.

3.25. Roadblocks

Used in tactics: **Arrest**, **Incrimination**

Roadblocks are temporary installations set up to control or block traffic on a road.

An adversary can set up roadblocks:

- As a planned measure, for example in the streets surrounding a planned protest, to control the flow of protesters.
- In response to an unexpected event, for example after an action in the hope of catching the people involved in the action.

In some contexts, the State systematically sets up roadblocks after certain events, such as high-profile robberies or prison escapes.

Mitigations

Attack (p. 143): You can attack roadblocks to disrupt them.

Careful action planning (p. 149): You can carefully plan an action to take into account the risk of roadblocks being set up after the action on roads surrounding the action site.

Repressive operations

Operation 8 (p. 209): On the morning of the October 15 raids, police set up a roadblock on the only road leading to an area where several raids were taking place.[81] For most of the day, cops staffing the roadblock searched, questioned, and photographed people passing on the road.[130]

3.26. Service provider collaboration

Used in tactic: **Incrimination**

Service provider collaboration is the process by which an entity that has information about you because it provides a service to you provides that information to an adversary. Service provider collaboration can provide both current and historical information.

The State can legally compel service providers to provide information, depending on the context. For example:

- Spain, a State with a high degree of control over companies located within its jurisdiction, can very easily compel Spanish mobile network operators to provide information on Spanish mobile network users.

[130] https://rnz.co.nz/news/national/135737/ipca-criticises-illegal-searches-during-urewera-raids

- Iran, a State with no diplomatic relations with Canada, cannot compel the Canada Revenue Agency to provide information on Canadian taxpayers.

Both non-State adversaries and the State can obtain service provider information through:

- Corruption: purchasing service provider information sold by corrupt individuals with access to the information (e.g., service provider employees, police officers).
- Data leaks:[131] obtaining service provider information through unauthorized exposure, disclosure, or loss of the information (e.g., a service provider database is hacked and an adversary buys it on the black market).

3.26.1. Mobile network operators

Mobile network operators can provide information about you to an adversary.

They can provide:

- Given a name: the phone numbers registered under that name.
- Given a phone number: the name under which the phone number is registered and the IMEI number[132] of the phone in which the phone number is used.
- Given an IMEI number: the phone number that is used in the phone with that IMEI number.

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

- The content of SMS and regular calls you make on your phone.
- The list of websites you visit on your phone.
- Your phone physical location.

[131] https://en.wikipedia.org/wiki/Data_breach

[132] An International Mobile Equipment Identity (IMEI) number is a number that uniquely identifies a phone.

- Metadata about your use of end-to-end encrypted messaging applications (e.g. when you use Signal and the approximate size of messages sent or received through Signal).

This means that any of the following conditions can allow an adversary, with the collaboration of mobile network operators, to access (current and historical) data and metadata about your phone activity:

- Knowing your name (if your phone is not **anonymous (p. 138)**).
- Knowing your phone number, which they can find by monitoring or seizing a phone in contact with yours, using an **IMSI-catcher (p. 129)**, or through advanced correlation techniques.[133]
- Knowing your phone IMEI number, which they can find by seizing your phone.

Mitigations

Anonymous phones (p. 138): You can use anonymous phones to make it harder for mobile network operators to provide useful information to an adversary.

Digital best practices (p. 152): You can follow digital best practices to make it harder for mobile network operators to provide useful information to an adversary. For example, you can:

- Not use a phone, or leave your phone at home.
- Use end-to-end encrypted messaging applications on your phone, instead of traditional SMS and calls.

Encryption (p. 161): You can encrypt "in-motion" data to make it harder for mobile network operators to provide useful information to an adversary.

Repressive operations

Case against Boris (p. 188): Investigators used the collaboration of mobile network operators to intercept calls from Boris's phone or the phones of people close to him.[22] They regularly listened to the intercepted calls in

[133] For example, if an adversary knows that you were in place A on Monday and in place B on Tuesday, and they know from cell tower data that a particular phone was the only phone that was also in place A on Monday and in place B on Tuesday, they can deduce the phone is yours.

real time and used information from the calls to adjust ongoing **physical surveillance (p. 99)** operations.

Repression against Zündlumpen (p. 191): Investigators used the collaboration of mobile network operators to:

- Intercept the calls of N.'s mother.[47] This allowed them to learn that N. was planning to visit her mother for Christmas, which allowed them to place N. under **physical surveillance (p. 99)**.
- Intercept the calls of people suspected of being close to N. and M.[9]

Search for a fugitive (p. 189): In 2022, investigators used the collaboration of mobile network operators to obtain information about the person's phone over a seven-month period, including:[7]

- Which other phones it had called and when.
- Which cell towers it had connected to and when. However, they did not obtain a more precise geolocation of the phone.

Case against Revolutionära fronten (p. 204): Investigators used the collaboration of mobile network operators to retroactively geolocate the phones of some of the defendants on the day of the Stockholm beating.[7] This showed that, on that day:

- Some phones had moved to Stockholm, suggesting that their owners had also traveled to Stockholm.
- Some other phones were turned off early in the morning and turned back on late at night, suggesting that their owners may have turned off their phones to avoid being tracked when going to Stockholm.

Mauvaises intentions (p. 208): Investigators used the collaboration of mobile network operators to link phone numbers to civil identities, to know which phone numbers were in contact with each other, to geolocate phones (both retrospectively and in real time) and to record phone calls.[37]

Arrest of Stecco (p. 194): Investigators used the collaboration of mobile network operators to:[17]

- Intercept the calls of more than 40 phones.
- Retroactively analyze the phone activity of 69 phones and one phone booth. In particular, once investigators thought they had found the general area where Stecco was living, they checked:

- Whether any of the 69 phones had called a phone in the area in the past 6 years.
- Whether Stecco had called a phone in the area in the 5 years before he went on the run.

Case against Amos Mbedzi (p. 207): Investigators found Mbedzi's and his comrades' phones at the bombing site, and used the collaboration of mobile network operators to retrospectively geolocate them and analyze their call history.[52] This showed that Mbedzi and his comrades regularly called each other and therefore knew each other, and had traveled together from South Africa to Eswatini the night before the bombing attempt.

Case against Louna (p. 182): Investigators used the collaboration of mobile network operators to geolocate approximately 30 phones and intercept their calls in real time.[7] In particular, investigators used the intercepted calls to:

- Hear about a meeting outside apartment buildings, set up physical surveillance of those buildings, and arrest two people who went to the meeting.
- Hear Louna make an appointment with a doctor, then contact the doctor to obtain Louna's personal information, including her address and phone number.

Bure criminal association case (p. 196): Investigators used the collaboration of mobile network operators to:[7]

- Establish links between people.
- Geolocate phones in real time.
- Record a large number of phone conversations, including conversations that took place between the moment a call was placed and the moment it was answered (i.e., while the phone was ringing).
- Identify the phone numbers that were active around Bure during three demonstrations that took place there in February, June, and August 2017, including 55 numbers that were active during all three demonstrations.

Operation 8 (p. 209): Investigators used the collaboration of mobile network operators to intercept calls and text messages.[6] The intercepted

text messages revealed the dates and locations of the "training camps" and who attended them.

Repression of the attack on Clarín's headquarters (p. 187): Investigators used the collaboration of mobile network operators to:[60]

- Analyze the activity of some of the defendants' phones at the time of the attack. Several phones were seemingly turned off shortly before the attack and turned back on shortly after, which was considered suspicious. For example, one phone was seemingly turned off ten minutes before the attack and turned back on approximately two hours after.
- Geolocate the phones of some of the defendants retroactively. This showed that:
  - One defendant spent time near the attack site the day before the attack.
  - One defendant was present at the attack site a few minutes before the attack.
- Intercept phone calls. In intercepted calls, some of the defendants expressed solidarity with those targeted by the investigation and concern about being targeted themselves.

December 8 case (p. 193): Investigators used the collaboration of mobile network operators to geolocate the phones of the defendants and of people close to them in real time and to record unencrypted phone conversations.[20] In particular:

- In one case, investigators could not determine the phone number used by one of the defendants, but had determined that the defendant often moved around with another person, so they geolocated the other person's phone in real time to locate the defendant.
- In one case, investigators followed one of the defendants as part of a **physical surveillance (p. 99)** operation, but lost sight of them. In the following hour, they geolocated the defendant's phone in real time to locate them. As a result, one hour after losing sight of the defendant, investigators regained sight of them and resumed the physical surveillance operation.

3.26.2. Other

Service providers other than mobile network operators can provide information about you to an adversary.

Stores

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

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

Additionally, physical stores can provide:

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

Banks

Banks can provide:

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

Internet service providers

Internet service providers can provide:

- If you follow **digital best practices (p. 152)** and use Tor: metadata about your Internet activity, such as when you use Internet.
- If you don't use Tor: your Internet activity, including the list of websites you visit.

Online services

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

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

Postal services

Postal services can allow an adversary to monitor your mail.

State institutions

State institutions can provide any information they have about you, including your address, tax records, health information, etc.

Mitigations

Anonymous purchases (p. 139): If you need to purchase an item in a store, you can purchase it anonymously to make it harder for an adversary to use the collaboration of the store to link your identity to the item.

Digital best practices (p. 152): You can follow digital best practices to make it harder for service providers to provide useful information to an adversary. For example, you can:

- Use Tor[103] to make it harder for your Internet Service Provider to provide useful information about your Internet activity to an adversary.
- Use trusted online services[134] that will refuse to comply with an adversary's requests to access your data, or build their service to make it technically impossible to comply with such requests.

Encryption (p. 161): You can encrypt "in-motion" data to make it harder for service providers to provide useful information to an adversary.

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

Case against Boris (p. 188): Investigators used the collaboration of an email provider to gain real-time access to an email address used by Boris: they were able to see emails sent and received in real time.

Repression against Zündlumpen (p. 191): Investigators used the collaboration of banks to:[47]

- Analyze the bank records of a suspected editor of the newspaper, including bank records as old as 8 years, to determine if the person had purchased printing equipment.
- Obtain, in real time, the locations of cash withdrawals made by N. When a cash withdrawal took place, investigators would send a patrol to the withdrawal location to try to locate N. However, this did not work, seemingly because the patrol always arrived too late.
- Reduce the maximum cash withdrawal limit of N. in order to force her to make more withdrawals and increase the opportunities of locating her.

Investigators asked several companies to provide information about N.:

- Mail order companies were asked to provide the shipping addresses she used.
- PayPal, Ebay, and similar companies were asked if she had an account with them and, if so, which addresses were associated with the account.
- The German national railway company (Deutsche Bahn) and the bus operator FlixBus were asked to provide information about her travels.
- Her former vocational school was asked to provide the list of participants in the school's courses, presumably to identify her possible contacts.

Search for a fugitive (p. 189): In 2022, investigators used the collaboration of service providers to obtain information about the person from:[7]

- Facebook, which provided the phone number that had been used to create an account on the social network Instagram. This account shared news about the struggle against the construction of a police training center. The phone number belonged to the person.

- The Supplemental Nutrition Assistance Program,[122] which provided a mailing address, a list of purchases made through the program in the past three months, an email address and a phone number.
- The company employing the person, which provided an email address and a phone number.
- The person's previous employer, who was interviewed but did not provide useful information.

Case against Revolutionära fronten (p. 204): Investigators used the collaboration of banks to obtain bank statements that showed one of the defendants had made a purchase at a Stockholm supermarket on the day of the Stockholm beating, suggesting that he was in Stockholm that day.[7]

Repression of Lafarge factory sabotage (p. 185): Investigators gave the serial number of a camera to the camera manufacturer, and the manufacturer gave them the name of the store where the camera was sold.[50] This helped investigators identify a person they accused of taking photos with the camera.

Arrest of Stecco (p. 194): Investigators used the collaboration of several companies:[17]

- The Italian national railway manager (RFI) provided CCTV footage from train stations, lists of tickets purchased from ticket machines, and searches made on ticket machines, even when no tickets were purchased.
- The Italian national railway operator (FSI) provided a list of fines on five different lines and a list of all tickets purchased under a given name in previous months. FSI also enabled an "automated alert" system that would have notified investigators when tickets were purchased under the name.
- Banks provided:
    - The bank records of 59 people, which investigators analyzed to determine if they contained "suspicious" transactions that could indicate financial support for Stecco.
    - The bank records of an anarchist journal, which investigators requested after seeing someone read an issue of the journal in CCTV footage.

- The classified ads website subito.it provided the IP addresses used to log into an account.
- An email service provider provided data related to email addresses.

Case against Peppy and Krystal (p. 183): A fireworks store provided investigators with records showing that Peppy had purchased fireworks from the store three days before the protest.[10]

Case against Louna (p. 182): Investigators used the collaboration of the hospital to:

- Learn that a person (Louna) was hospitalized for burns.[7]
- Obtain Louna's medical file.
- Seize Louna's clothing while she was hospitalized.[80]
- Obtain the phone number of someone close to Louna that Louna had given to the hospital.
- Obtain CCTV footage from the hospital.
- Obtain information from the hospital's parking payment system.
- Learn the time and place of an appointment Louna had at the hospital a few days after the arson.

Investigators also used the collaboration of several State institutions:

- The Agence nationale des titres sécurisés (ANTS, *National agency for secured documents*) provided scans of identity documents and applications for renewal of identity documents.
- Health insurance organizations provided the personal information of people under investigation and their partners.
- The tax authorities provided the purchase and sale files of houses of Louna's parents and grandparents.

Investigators used the collaboration of several companies:

- Banks provided:
  - Bank information of several people, including many members of Louna's family.
  - IP addresses used to make online bank transfers.
  - Locations where people had withdrawn cash.

- An insurance company provided a person's address and list of roommates.
- The highway operator Vinci provided CCTV footage of highway toll booths.
- The French national railway company (SNCF) provided information about people who had booked seats next to people under investigation, including their photos and bank information.
- The carpooling service BlaBlaCar provided information about people who had used the service, including their photos, bank information, and the trips they had taken.
- The car manufacturer Stellantis provided the IMSI[135] and IMEI[132] numbers of a car's embedded location system. However, investigators were unable to locate the car because, for some unknown reason, it did not transmit its location.

Investigators asked a social housing landlord and a real estate agency to provide them with access cards to apartment buildings.

Bure criminal association case (p. 196): Investigators used the collaboration of banks to obtain the bank records of organizations fighting against Cigéo.[7] The bank records of one organization included a 500€ transfer entitled "*participation manif 18 fev*" ("*contribution to the February 18 demonstration*"), in reference to a demonstration in which people attacked a building associated with Cigéo.

The owner of a supermarket in a town about 20 km from Bure told investigators that he had seen customers buying an unusually large amount of denatured alcohol (15 liters), and gave the receipt to the investigators.

Operation 8 (p. 209): Investigators used the collaboration of service providers to obtain information on people from many different sources, including:[6]

- Court records.
- Birth, death, and marriage records.
- Electoral registers.

[135] An International Mobile Subscriber Identity (IMSI) number is a number that uniquely identifies a SIM card.

- Records from Work and Income New Zealand (WINZ),[136] the State agency that provides social services.
- Property ownership records.
- Vehicle ownership records.
- Car registration records.
- Power company client records.
- Bank records.
- Overseas travel movements, in one case dating back to 1983.
- Trade Me, New Zealand's largest online auction website.

Investigators used the collaboration of the New Zealand Army to find out who, in a list of 58 people, had served in the military, presumably to identify who had military experience that they could use to contribute to the "training camps."

Repression of the attack on Clarín's headquarters (p. 187): One defendant was identified because he was seen on CCTV footage boarding a bus and he used his partner's electronic bus card to board the bus—investigators presumably obtained his partner's name using the collaboration of the entity that manages the bus card system.[60]

3.27. Targeted digital surveillance

Used in tactic: **Incrimination**

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

Extremely advanced techniques exist[137] in the arsenal of nation-State actors, but the focus here is on techniques that are more likely to be used against anarchists and other rebels.

See the "Digital surveillance" topic.[102]

[136] Now called the Department of Work and Income.

[137] https://anonymousplanet.org/guide/some-advanced-targeted-techniques

3.27.1. Authentication bypass

Authentication bypass is the process by which an adversary bypasses the **Full Disk Encryption (p. 161)** that protects access to a digital device. An adversary can achieve authentication bypass through human error, weak passwords, or technical exploits.

An adversary can achieve authentication bypass in the following ways:

- Accessing the device while it is turned on (and therefore its encryption is not effective).
- Finding the encryption password written down somewhere.
- Making the device owner provide the encryption password by using **interrogation techniques (p. 83)** including, in some contexts, **physical violence (p. 108)**.
- Visual interception: watching the device owner type the encryption password through a **hidden camera (p. 23)** or an **infiltrator (p. 78)** or **informant (p. 80)**.
- Brute force: guessing the encryption password through repeated, automated authentication attempts.
- Compromising the device either through remotely-installed **malware (p. 131)** or **physical access (p. 135)**.
- Exploiting a flaw at the implementation level of the encryption process.

Mitigations

Bug search (p. 147): Before entering a password in a room where **covert video surveillance devices (p. 23)** may be present, you can conduct a bug search to locate such devices and eventually remove them.

Digital best practices (p. 152): You can follow digital best practices, and in particular use security-oriented operating systems with Full Disk Encryption (FDE) and strong passwords, to make it harder for an adversary to bypass authentication on your digital devices. For example:

- On computers, you can use the Linux FDE called LUKS, which is used by many Linux systems, such as Debian[138] and Tails,[57] and

which the forensics department of the German federal police was unable to decrypt after a year of effort.[139]

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

Tamper-evident preparation (p. 179): You can use tamper-evident preparation to detect when a device has been **physically accessed (p. 135)**.

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

Repressive operations

Repression against Zündlumpen (p. 191): In some of the raids, police seized smartphones immediately after entering and plugged them into power banks, presumably to prevent them from shutting down and reverting to an encrypted state.[141]

The February arrests of N. and M. took place in a public library, while N. and M. were using a computer.[28] Police officers wearing civilian clothes waited until N. and M. had unlocked the computer to reveal themselves and make the arrest, presumably to access the computer while it was unlocked.

Repression of Lafarge factory sabotage (p. 185): Investigators seized several encrypted smartphones in the raids and attempted to access their encrypted data, with varying results depending on the phone:[50]

- For the iPhones that were seized turned on, they exploited the security vulnerabilities that exist when they are turned on to bypass their encryption and access the encrypted data.

---

[138] https://debian.org

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

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

[141] 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

- For all Android phones (whether recovered on or off) and one iPhone seized off, they extracted the phones' encrypted partitions and attempted to brute force them from a computer.

Arrest of Stecco (p. 194): Investigators found the PIN code of the smartphone of someone under surveillance when a camera hidden in a car captured the person entering the code.[17]

Investigators attempted to find the password of a Tails system through brute force using a software called "bruteforce-luks."

2011-2013 case against Jeremy Hammond (p. 205): Investigators bypassed the authentication of Jeremy Hammond's encrypted laptop, that they had seized in the March 2012 raid.[142] They seemingly achieved the bypass by guessing the laptop's password, which was a very simple password—either "chewy123"[143] or "chewy12345".[144]

Bure criminal association case (p. 196): Investigators bypassed the authentication of five encrypted hard drives found in raids:[7]

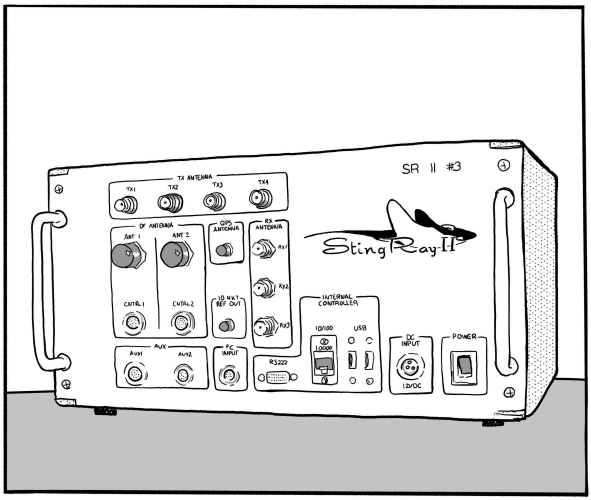
- One hard drive by using the very simple password "stopcigeo", which they presumably guessed.
- One hard drive by using a password they found on a post-it note under the computer containing the hard drive.
- One hard drive by using a password given to them in custody by the owner of the computer containing the hard drive.
- Two hard drives by using passwords they found in a text document on a previously decrypted hard drive.

[142] https://apnews.com/domestic-news-domestic-news-general-news-abae6d15cbf04d75bbbc58225a470f98

[143] According to press reports.

[144] According to *American Kingpin* (Nick Bilton, 2017).

3.27.2. IMSI-catcher



An IMSI-catcher (also known as a *Stingray*) is a device used to collect information about all mobile phones that are turned on in a limited area (from a few meters to several hundred meters) around it. A passive IMSI-catcher simply listens to the traffic, while an active IMSI-catcher acts as a "fake" cell tower between the phones and the legitimate cell towers.

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

- Their numbers.
- Their IMSI[135] and IMEI[132] numbers.
- Data and metadata about their activity: the content of SMS and regular calls, the list of visited websites, metadata about the use of end-to-end encrypted messaging applications (e.g. when Signal is used and the approximate size of messages sent or received through Signal).

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

- At a public demonstration, to record the phone numbers of all the phones present at the demonstration and later obtain the names

associated with those phone numbers through the **collaboration of mobile network operators (p. 114)**.

- As part of a **physical surveillance (p. 99)** operation to record the target's phone number or the phone numbers of people in contact with the target.

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

- To record the activity of a target phone without requiring the collaboration of the mobile network operator (which, in some contexts, may require a warrant).
- To record the activity of a target phone when the adversary knows where the phone is being used, but doesn't know its phone number.

See the "IMSI-catchers" topic.[145]

Mitigations

Bug search (p. 147): You can conduct a bug search to detect the presence of an IMSI-catcher.

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

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

Encryption (p. 161): You can encrypt a phone "in-motion" data so that if the data is collected by an IMSI-catcher, it cannot be analyzed. For example, you can use end-to-end encrypted messaging applications instead of legacy texts and calls for your phone communications.

Repressive operations

Case against Boris (p. 188): Investigators used IMSI-catchers during **physical surveillance (p. 99)** operations to identify the phone numbers

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

of people Boris was meeting with—and then identified those people by asking mobile network operators for the names corresponding to the phone numbers.[22]

Repression against Zündlumpen (p. 191): Investigators used an IMSI-catcher to identify the phone number of N.'s mother. They used it both at the mother's home and at her workplace: the correlation of the two uses allowed them to identify the phone number.[47]

Bure criminal association case (p. 196): Investigators used IMSI-catchers to identify the phone numbers of people who lived in places associated with the struggle against Cigéo or who participated in demonstrations.[7]

December 8 case (p. 193): Investigators used an IMSI-catcher during **physical surveillance (p. 99)** operations to identify the phone numbers used by some of the defendants.[20]

3.27.3. Malware

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

Malware can be installed on a device:

- Remotely, with interaction from the target. This is typically done through phishing,[146] which often requires the target to open a malicious file or link.
- Remotely, without interaction from the target. This type of malware is often very expensive for the adversary. An example of malware that has been able to install itself without interaction from the target is Pegasus.[147]
- By **physically accessing (p. 135)** the device.

[146] https://en.wikipedia.org/wiki/Phishing
[147] https://en.wikipedia.org/wiki/Pegasus_(spyware)

See also:

- "It Could Be Harmful! Spyware Installation Through Social Engineering Attacks in Italy"[148] for an example of malware installed through phishing.
- The "Targeted malware" topic.[149]

Mitigations

Compartmentalization (p. 151): If an adversary installs malware on a Tails[57] USB stick or a Qubes OS[150] virtual machine that you use for different digital identities, they can tie the different identities together. To mitigate this, you can use different Tails USB sticks or Qubes OS virtual machines for different digital identities.

Computer and mobile forensics (p. 152): You can use computer and mobile forensics to detect traces of malware on a device on which malware is or was installed.

Digital best practices (p. 152): You can follow digital best practices to make it harder for an adversary to install malware on your digital devices. For example, you can:

- Follow best practices against phishing to make it harder for an adversary to trick you into installing malware on your digital devices.
- Use Tor[103] or a VPN to make it harder for an adversary to remotely install malware on your digital devices through a targeted network injection.[151]

Encryption (p. 161): You can encrypt "in-motion" data to make it harder for an adversary to install malware through *network packet injection*, an installation vector for some malware, such as Pegasus.[152]

[148] https://notrace.how/resources/#could-be-harmful
[149] https://notrace.how/resources/#topic=targeted-malware
[150] https://qubes-os.org
[151] https://en.wikipedia.org/wiki/Packet_injection
[152] https://forbiddenstories.org/about-the-pegasus-project

Scripta Manent (p. 210): Malware was installed on the computer of one of the defendants.[153] The malware, which was installed remotely over the Internet, targeted a Windows computer and was capable of recording text typed on the keyboard, taking periodic screenshots, and recording communications sent and received to and from the computer.

Repression of Lafarge factory sabotage (p. 185): Investigators made five requests to remotely install spyware.[50] Of these, one installation was successful (on an iPhone SE 2020) and provided access to a Signal group conversation.

Arrest of Stecco (p. 194): Investigators attempted to install malware on the smartphone of someone under surveillance.[17] They sent the person an SMS with a link. If the person had clicked on the link, the malware would have been installed, allowing investigators to listen to conversations through the smartphone's microphone. But the person did not click on the link, so the malware was not installed.

3.27.4. Network forensics

Network forensics is the monitoring and analysis of network traffic.

Network information is volatile, it is designed to be transmitted and then lost, so monitoring it requires a proactive approach. Many countries have built network monitoring centers that store massive amounts of network information for days, months, or years to be analyzed later. An adversary can also monitor your network traffic with the **collaboration of your Internet Service Provider (p. 119)**, by compromising your home router with **malware (p. 131)**, or by monitoring your wired or wireless network connection from a surveillance vehicle outside your home.

Because most websites, email providers, and messaging applications use SSL/TLS encryption (the "s" in "https"), an adversary monitoring your network traffic usually knows what websites you visit, but not what you do on those websites. If you use Tor,[103] an adversary monitoring your network

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

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

Tor is vulnerable to correlation attacks, but such attacks are difficult to set up even for powerful adversaries. An example of a successful correlation attack is the prosecution of anarchist hacker Jeremy Hammond: the times when the alias he used in chat rooms was "online" (obtained through network traffic analysis) were correlated with the times when a **physical surveillance (p. 99)** operation observed him at home to prove that the alias belonged to him.[154]

Mitigations

Compartmentalization (p. 151): An adversary can establish links between different digital identities through the footprints left by their network traffic. To mitigate this, you can compartmentalize different digital identities by:

- Using Tails[57] and rebooting between each session.
- Using Qubes OS[150] with different Whonix[155] virtual machines that you use non-simultaneously.

Digital best practices (p. 152): You can follow digital best practices, and in particular use Tor,[103] to make it harder for an adversary to monitor and analyze your network traffic.

Encryption (p. 161): You can encrypt "in-motion" data to make it harder for an adversary to analyze the data with network forensics.

Repressive operations

2011-2013 case against Jeremy Hammond (p. 205): For several days, investigators analyzed the network traffic of the router used by Jeremy Hammond to establish a correlation between:[93]

- The times when the traffic showed usage of the Tor network.
- And the times when Jeremy Hammond's online persona was reported as being online by the informant Sabu.

---

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

[155]https://whonix.org

3.27.5. Physical access

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

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

- Computers, phones, and storage devices (e.g. hard drives, USB sticks, SD cards).
- Printers, cameras, "smart" TVs.
- Vehicles. For example, navigation systems[156] in modern vehicles can store records of the vehicle location.

If an adversary physically accesses a device, they can:

- Read the device unencrypted data, or its encrypted data if it is turned on (and therefore its **encryption (p. 161)** is not effective).
- Compromise the device with **malware (p. 131)**.
- Compromise the device with a hardware keylogger.[157]

An adversary can physically access a device:

- During a **house raid (p. 72)** or a **covert house visit (p. 15)**.
- After arresting you if you have the device on you.
- During a border control.
- Through an **infiltrator (p. 78)** or **informant (p. 80)** that has access to the device.

Mitigations

Computer and mobile forensics (p. 152): You can use computer and mobile forensics to detect when a device has been physically accessed by an adversary.

Digital best practices (p. 152): You can follow digital best practices to mitigate the risk of an adversary physically accessing your digital devices.

[156] https://en.wikipedia.org/wiki/Automotive_navigation_system
[157] https://en.wikipedia.org/wiki/Hardware_keylogger

For example, if you are going to an event or demonstration and you think that you could be arrested, you should not take your phone with you.

Network map exercise (p. 168): An adversary could physically access your digital devices through an **infiltrator (p. 78)** or **informant (p. 80)**. To mitigate this, you can conduct a network map exercise to help you decide who you trust to access your digital devices.

Physical intrusion detection (p. 170): You can use physical intrusion detection to detect when a space has been physically accessed by an adversary.

Tamper-evident preparation (p. 179): You can use tamper-evident preparation to detect when something has been physically accessed by an adversary.

4. Mitigations

4.1. Anonymous dress

Techniques addressed by this mitigation:

Forensics > Facial recognition (p. 52)
Forensics > Gait recognition (p. 57)
Forensics > Trace evidence (p. 69)
Mass surveillance > Civilian snitches (p. 85)
Mass surveillance > Video surveillance (p. 91)
Physical surveillance > Aerial (p. 100)
Physical surveillance > Overt (p. 108)

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. 147)**).

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. 139)** 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 (p. 95)
Service provider collaboration > Mobile network operators (p. 115)

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. 139)** 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 (p. 114)**.

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 (p. 95)**—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"[158] on the dangers of using a phone.
- Burner Phone Best Practices[159] for more information on burner phones.

4.3. Anonymous purchases

Techniques addressed by this mitigation:

Forensics > Arson (p. 39)
Forensics > Ballistics (p. 41)
Forensics > Trace evidence (p. 70)
Mass surveillance > Video surveillance (p. 91)

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

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 (p. 34)**) 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 (p. 119)**, 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. 180)**), and do not bring a phone.
- Conduct **anti-surveillance (p. 141)** before going to the store.
- Use some level of **anonymous dress (p. 137)** 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.

See also

See PRISMA[70] for more details on physical anonymous purchases.

4.4. Anti-surveillance

Techniques addressed by this mitigation:

Physical surveillance > Aerial (p. 100)
Physical surveillance > Covert (p. 103)

Anti-surveillance is the practice of taking active measures to evade ("shake off") a **mobile physical surveillance operation (p. 101)**.

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 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[119] about the principles and techniques of anti-surveillance.
- The "Physical surveillance" topic.[121]
- The related mitigation **Surveillance detection (p. 176)**.

4.5. Attack

Techniques addressed by this mitigation:

Alarm systems (p. 12)
Guards (p. 71)
Increased police presence (p. 77)
Infiltrators (p. 79)
Informants (p. 80)
Mass surveillance > Civilian snitches (p. 85)
Mass surveillance > Police files (p. 89)

Mass surveillance > Video surveillance (p. 92)
Physical surveillance > Aerial (p. 100)
Police patrols (p. 112)
Roadblocks (p. 113)

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[160] and P25[161] 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.

4.6. Avoiding self-incrimination

Techniques addressed by this mitigation:

Door knocks (p. 31)
Forensics > Digital (p. 50)
ID checks (p. 77)
Interrogation techniques (p. 84)
Mass surveillance > Mass digital surveillance (p. 88)
Network mapping (p. 95)
Open-source intelligence (p. 97)

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

[160] https://en.wikipedia.org/wiki/TETRA
[161] https://en.wikipedia.org/wiki/Project_25

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[162] on how to resist police interrogation techniques.

Need-to-know principle

Apply the **need-to-know principle (p. 167)**. 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. 152)**. 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.[163]

[162] https://notrace.how/resources/#police-interrogation

4.7. Background checks

Techniques addressed by this mitigation:

Infiltrators (p. 79)
Informants (p. 80)

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:

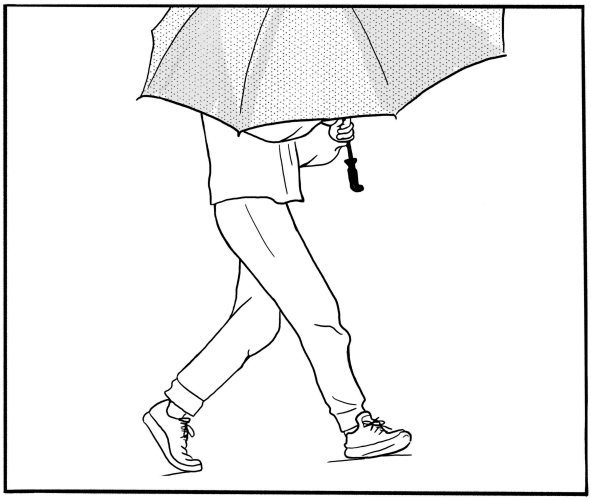
- Confidence, Courage, Connection, Trust[164] on the use of ID checks to verify that someone is who they say they are.
- Handbook for Exposing an Undercover Cop[165] on a method for identifying, investigating and exposing undercover cops, including through using background checks.

[163] https://rosecitycounterinfo.noblogs.org/2022/08/uprising-lessons
[164] https://notrace.how/resources/#confidence
[165] https://notrace.how/resources/#handbook-undercover-cop

4.8. Biometric concealment

Techniques addressed by this mitigation:

Forensics > Facial recognition (p. 52)
Forensics > Gait recognition (p. 57)
Forensics > Handwriting analysis (p. 61)
Forensics > Linguistics (p. 63)
Mass surveillance > Video surveillance (p. 92)



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[58] and the chapter "Traces" in PRISMA.[70]

4.9. Bug search

Techniques addressed by this mitigation:

Covert surveillance devices > Audio (p. 19)
Covert surveillance devices > Location (p. 22)
Covert surveillance devices > Video (p. 24)
Targeted digital surveillance > Authentication bypass (p. 126)
Targeted digital surveillance > IMSI-catcher (p. 130)

A bug search is the active process of trying to detect the presence of **covert surveillance devices (p. 16)** 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. 169)**.

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. 180)**, 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. 176)**.

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,[12] 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 (p. 29)
Forensics > Arson (p. 39)
Forensics > DNA (p. 45)
Forensics > Fingerprints (p. 54)
Forensics > Gait recognition (p. 57)
Forensics > Trace evidence (p. 70)
Increased police presence (p. 78)
Mass surveillance > Civilian snitches (p. 85)
Police patrols (p. 112)
Roadblocks (p. 113)

When planning an action, careful action planning is the sensible development of the action plan. It follows **reconnaissance (p. 173)**.

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. 141)** prior to the action meeting point?

4.11. Clandestinity

Techniques addressed by this mitigation:

Covert house visit (p. 15)
House raid (p. 73)

Clandestinity is the process of breaking away from your established identity and begin a new life with a **fake identity (p. 162)**.

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.[166]

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

4.12. Compartmentalization

Techniques addressed by this mitigation:

Network mapping (p. 95)
Targeted digital surveillance > Malware (p. 132)
Targeted digital surveillance > Network forensics (p. 134)

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[57] USB sticks or Qubes OS[150] virtual machines for different digital identities. This way, if an adversary compromises one stick or virtual machine with **malware (p. 131)**, 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. 167)** 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. 141)** 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 (p. 132)
Targeted digital surveillance > Physical access (p. 135)

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 organizations AccessNow[167] or Amnesty International,[168] 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[169] page on Privacy Guides.
- Practical Linux Forensics[170] for a comprehensive introduction to the skill set on Linux, the platform most relevant to anarchists and other rebels.

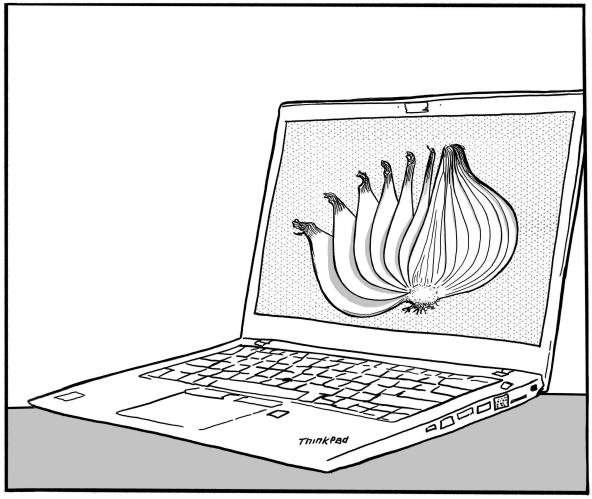
4.14. Digital best practices

Techniques addressed by this mitigation:

Alarm systems (p. 13)
Biased interpretation of evidence (p. 13)
Covert surveillance devices > Video (p. 24)
Door knocks (p. 32)
Doxing (p. 32)

[167] https://accessnow.org/help
[168] https://securitylab.amnesty.org/get-help
[169] https://privacyguides.org/en/device-integrity
[170] https://notrace.how/resources/#linux-forensics

Forensics > Digital (p. 50)
Mass surveillance > Mass digital surveillance (p. 89)
Network mapping (p. 95)
Service provider collaboration > Mobile network operators (p. 115)
Service provider collaboration > Other (p. 120)
Targeted digital surveillance > Authentication bypass (p. 126)
Targeted digital surveillance > Malware (p. 132)
Targeted digital surveillance > Network forensics (p. 134)
Targeted digital surveillance > Physical access (p. 135)



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[171] 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"[158] on the dangers of using a phone.

Use security-oriented operating systems

Use:

- Debian[138] or Qubes OS[150] for daily computer use. See AnarSec's guide "Qubes OS for Anarchists"[172] on Qubes OS.
- Tails[57] 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"[173] and "Tails Best Practices".[174]
- GrapheneOS[171] for phones. See AnarSec's guide "GrapheneOS for Anarchists".[175]

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. 161)** 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

[171] https://grapheneos.org
[172] https://anarsec.guide/posts/qubes
[173] https://anarsec.guide/posts/tails
[174] https://anarsec.guide/posts/tails-best
[175] https://anarsec.guide/posts/grapheneos

KeePassXC[176]—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[177] passwords of 5 to 10 words.[178] You can generate such passwords with KeePassXC (select the "Passphrase" tab when generating a password) or with physical dice.[179] 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

[176]https://keepassxc.org

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

[178]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*.

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

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[103] 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 (p. 131)**).

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.
- 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.[180] You should not connect to a VPN *after* Tor unless you really know what you are doing.[181]

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. 166)** applications such as Cwtch[182] or Briar.[183] Otherwise, use metadata-resistant applications such as SimpleX[184] or Signal.[185]
- 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.[134]

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"[186] for recommendations of end-to-end messaging applications.

[180] 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.

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

[182] https://cwtch.im

[183] https://briarproject.org

[184] https://simplex.chat

[185] https://signal.org

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

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. 161)**. 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 (p. 72)** 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. 179)**.

Buy your devices anonymously

Buying digital devices anonymously (p. 139) 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 (p. 50)**. 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

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. 161)** using a strong password, an adversary could **bypass the encryption (p. 126)**.
- Modern storage devices can store a hidden copy of their data in *spare memory cells*,[187] 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 (p. 131)** 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[188] on the measures you can take against phishing.
- **Doxing (p. 32)** is when an adversary publishes your personal information without your consent. See Doxcare: Prevention and Aftercare for Those Targeted by Doxxing and Political Harassment[189] on the measures you can take against doxing.

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

4.15. DNA minimization protocols

Technique addressed by this mitigation:

Forensics > DNA (p. 45)

DNA minimization protocols allow you to manipulate objects while minimizing the amount of **DNA (p. 42)** 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"[42] for protocol suggestions, and the "DNA" topic.[43]

4.16. Encryption

Techniques addressed by this mitigation:

Forensics > Digital (p. 51)
Mass surveillance > Mass digital surveillance (p. 89)
Service provider collaboration > Mobile network operators (p. 115)
Service provider collaboration > Other (p. 120)
Targeted digital surveillance > IMSI-catcher (p. 130)
Targeted digital surveillance > Malware (p. 132)
Targeted digital surveillance > Network forensics (p. 134)

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. 152)**. When the device is turned off, its data is encrypted; when you turn it on and enter the decryption key, its data is decrypted until it is turned off. If a device with FDE enabled is seized by an adversary during an arrest, **house raid (p. 72)**, or **covert house visit (p. 15)** while it is turned off, the adversary will not be able to access its data (unless they **bypass its authentication (p. 126)**).

You can encrypt "in motion" data by using Tor[103] or a Virtual Private Network (VPN) for your Internet activity, and by using **end-to-end encrypted messaging applications (p. 152)** 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. 169)**.

4.17. Fake ID

Techniques addressed by this mitigation:

ID checks (p. 77)
Network mapping (p. 95)

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.

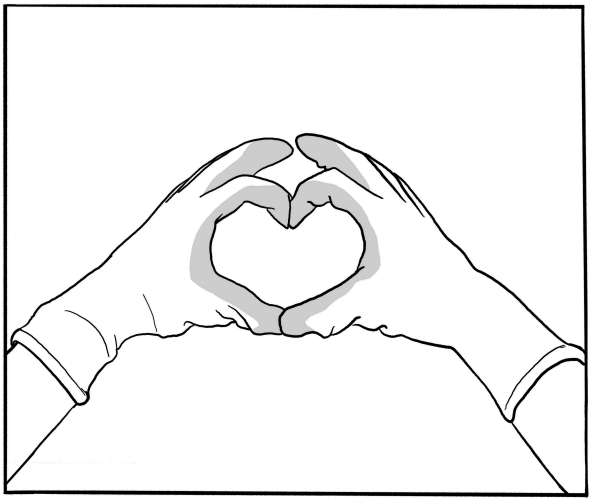
You can use a fake ID:

- To mitigate **network mapping (p. 95)** or avoid arrest in the event of an **ID check (p. 76)**.
- To establish a **safe house (p. 174)**.
- To take the path of **clandestinity (p. 150)**.

4.18. Gloves

Techniques addressed by this mitigation:

Forensics > DNA (p. 45)
Forensics > Fingerprints (p. 55)



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[190]).
- Do not use work gloves by themselves because they are generally permeable, and can let your sweat (and therefore your DNA) out.

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

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.[191]
- 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. 160)**.

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. 137)**.

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.

[191] 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.

- 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.[61]
- Handschuhe[192] (in German).

4.19. Masking your writing style

Technique addressed by this mitigation:
Forensics > Linguistics (p. 63)

Masking your writing style is the practice of altering the way you write to counter author identification by **forensic linguistics (p. 62)**.

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 (p. 72)** or **covert house visit (p. 15)**, and generally avoid publishing texts in your name throughout your life.

See Counteracting Forensic Linguistics[193] and Who wrote that?[68]

---

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

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

4.20. Metadata erasure and resistance

Technique addressed by this mitigation:

Forensics > Digital (p. 51)

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[194] that identifies the make and model of the printer that printed it.

Metadata erasure

For digital files, metadata erasure can be accomplished using MAT2[195] or similar software. Some **security-oriented operating systems (p. 152)** include metadata erasure tools by default.

Metadata resistance

Examples of metadata resistance include:

- Using a dedicated operating system (e.g. a Tails[57] 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. 152)**.

[194] https://eff.org/issues/printers
[195] https://github.com/tpet/mat2

See also

See AnarSec's guide "Remove Identifying Metadata From Files"[196] on how to remove metadata from digital files.

4.21. Need-to-know principle

Techniques addressed by this mitigation:

Biased interpretation of evidence (p. 13)
Infiltrators (p. 79)
Informants (p. 80)
Network mapping (p. 95)
Physical violence (p. 109)

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.

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

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:

- Secrets And Lies[197] about the effects that secrecy can have on an individual and collective level.
- The "Security culture" topic.[198]

4.22. Network map exercise

Techniques addressed by this mitigation:

Infiltrators (p. 79)
Informants (p. 81)
Network mapping (p. 95)
Targeted digital surveillance > Physical access (p. 136)

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 (p. 78)** 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

[197] https://notrace.how/resources/#secrets-lies
[198] https://notrace.how/resources/#topic=security-culture

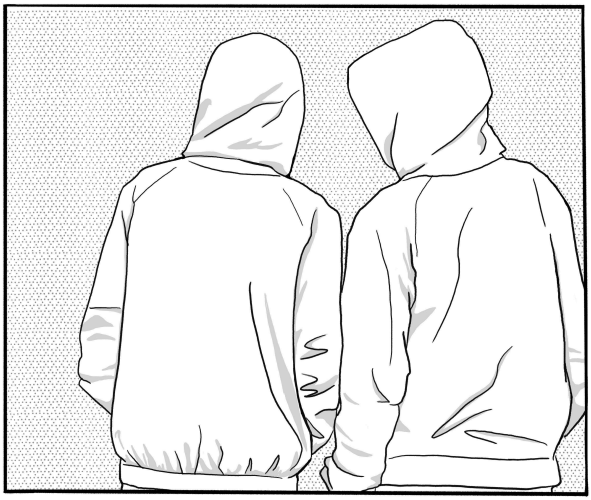
your level of security with all the people in your network, from which you draw a map that distinguishes the people you trust from the people you would like to know more about. It is designed to be done in times of relative calm.

For instructions on how to do this, see Stop hunting sheep: a guide to creating safer networks.[84] Such a network map would be invaluable to an adversary—it is essentially what they construct during **network mapping (p. 95)**—so it should be burned immediately after use.

4.23. Outdoor and device-free conversations

Techniques addressed by this mitigation:

Covert surveillance devices > Audio (p. 19)
Mass surveillance > Video surveillance (p. 92)



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 (p. 16)**.

- Electronic devices can be infected with **malware (p. 131)** that can turn them into covert microphones.

Outdoor conversations can be recorded with covert microphones or long-range parabolic microphones during a **physical surveillance (p. 99)** operation (with ranges of up to 300 meters). For example, in Italy in 2019[199] 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. 166)** 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.[198]

4.24. Physical intrusion detection

Techniques addressed by this mitigation:

Covert house visit (p. 15)
Covert surveillance devices > Audio (p. 19)
Covert surveillance devices > Location (p. 22)
Covert surveillance devices > Video (p. 24)
Evidence fabrication (p. 33)
Targeted digital surveillance > Physical access (p. 136)

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 (p. 15)**. 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.

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

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 (p. 16)
House raid (p. 73)

Preparing for house raids is the process of taking precautionary measures to minimize the impact of a potential **house raid (p. 72)** or **covert house visit (p. 15)**.

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. 161)**, 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. 174)**, 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 (p. 135)** an electronic device during a covert house visit, you can use **tamper-evident preparation (p. 179)**.

4.26. Preparing for repression

Techniques addressed by this mitigation:

House raid (p. 73)
Physical violence (p. 109)

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[200] where he secluded himself in a house in the mountains for a month to prepare for the possibility of his imprisonment.

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

4.27. Prisoner support

Technique addressed by this mitigation:

Informants (p. 81)

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 (p. 13)
Guards (p. 72)
Mass surveillance > Video surveillance (p. 92)
Police patrols (p. 112)

Reconnaissance is the gathering of information about the target of an action. It precedes **action planning (p. 149)**. 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 (p. 90)** coverage and a suitable place to change clothing before the action.
- Inspecting the action site itself, looking for surveillance cameras, **guards (p. 71)**, **alarm systems (p. 12)** and opportunities to attack the target.

When conducting physical reconnaissance, you can:

- Practice **anti-surveillance (p. 141)** to counter the risk of physical surveillance.
- **Dress anonymously (p. 137)** 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. 152)**.

4.29. Stash spot or safe house

Techniques addressed by this mitigation:

Covert house visit (p. 16)
Covert surveillance devices > Video (p. 24)
Forensics > Ballistics (p. 41)
Forensics > Trace evidence (p. 70)
House raid (p. 73)

Stash spots and safe houses are two ways to store incriminating materials. If incriminating materials are stored in a stash spot or safe house instead of in your home, they won't be found by an adversary in the event of a **house raid (p. 72)** or a **covert visit (p. 15)** 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. 160)** 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. 162)** 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.[24] Because of this, when accessing a stash spot or safe house, you can:

- Practice **anti-surveillance (p. 141)** to counter the risk of physical surveillance.
- **Dress anonymously (p. 137)** to counter the risk of being observed or recorded.
- Practice **tamper-evident preparation (p. 179)** to ensure that the stash spot or safe house hasn't been accessed by an adversary.

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

See "Security Culture and Safe Houses: Sustaining the Network, Nurturing Continuity"[201] 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 (p. 25)
Physical surveillance > Aerial (p. 100)
Physical surveillance > Covert (p. 103)

Surveillance detection is the practice of detecting if you are under **physical surveillance (p. 99)**, 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[119] about the principles and techniques of surveillance detection.
- The "Physical surveillance" topic.[121]
- The related mitigation **Anti-surveillance (p. 141)**.

4.31. Tamper-evident preparation

Techniques addressed by this mitigation:

Targeted digital surveillance > Authentication bypass (p. 127)
Targeted digital surveillance > Physical access (p. 136)

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 when something has been **physically accessed (p. 135)** by an adversary.

Tamper-evident preparation can be used:

- To detect if an adversary has accessed an electronic device during a **covert house visit (p. 15)** (in which case they may have installed **malware (p. 131)** on the device).
- To detect if an adversary has accessed a **stash spot or safe house (p. 174)**.

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"[202] on how to use tamper-evident preparation for electronic devices.

4.32. Transportation by bike

Techniques addressed by this mitigation:

Covert surveillance devices > Location (p. 22)
Mass surveillance > Video surveillance (p. 92)
Physical surveillance > Covert (p. 103)

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 (p. 90)** than cars: the make and model of a bike can be obscured and bikes usually have no license plates.

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

- It is harder for a **physical surveillance (p. 99)** 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. 176)** and **anti-surveillance (p. 141)** 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.[203]
- There are far fewer places to install a **tracking device (p. 21)** on a bike than on a car, and when you **search (p. 147)** a bike, you can tell with a high degree of confidence whether a tracking device is present or not.

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

5. Repressive operations

5.1. Case against Louna

Country: **France (p. 215)**
Date: **2024 - ?**
Techniques used:

- **Covert surveillance devices > Audio (p. 20)**
- **Covert surveillance devices > Location (p. 23)**
- **Covert surveillance devices > Video (p. 26)**
- **Forensics > Arson (p. 40)**
- **Forensics > DNA (p. 47)**
- **Guards (p. 72)**
- **House raid (p. 74)**
- **Mass surveillance > Civilian snitches (p. 86)**
- **Mass surveillance > Video surveillance (p. 93)**
- **Physical surveillance > Covert (p. 105)**
- **Service provider collaboration > Mobile network operators (p. 117)**
- **Service provider collaboration > Other (p. 123)**

On the night of May 4 to May 5, 2024, an excavator was set on fire at the construction site of a highway project.[80] 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.[204] After her arrest, she claimed responsibility for the degradations against the excavator. She is currently under judicial supervision pending trial.

5.2. Berlin 2023 railway conspiracy case

Country: **Germany (p. 215)**
Date: **2023 - 2024**
Technique used:

Physical surveillance > Aerial (p. 100)

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.[116] 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.[205]

5.3. Case against Peppy and Krystal

Country: **United States (p. 216)**
Date: **2023 - ?**
Techniques used:

Covert house visit (p. 16)
Mass surveillance > Video surveillance (p. 93)
Physical surveillance > Covert (p. 104)
Service provider collaboration > Other (p. 123)

In 2023, the home of Peppy and Krystal was raided, and both were arrested a month later.[206] 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.[10]

---

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

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

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

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.

5.4. Case against Ruslan Siddiqi

Country: **Russia (p. 216)**
Date: **2023 - 2025**
Techniques used:

- **Forensics > DNA (p. 49)**
- **Forensics > Trace evidence (p. 70)**
- **Interrogation techniques (p. 84)**
- **Mass surveillance > Civilian snitches (p. 87)**
- **Mass surveillance > Video surveillance (p. 94)**
- **Physical violence (p. 110)**

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.[100] 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.[54]

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.[207]

5.5. Repression of Lafarge factory sabotage

Country: **France (p. 215)**
Date: **2022 - ?**
Techniques used:

- **Forensics > DNA (p. 47)**
- **House raid (p. 74)**
- **Mass surveillance > Video surveillance (p. 93)**
- **Open-source intelligence (p. 98)**
- **Service provider collaboration > Other (p. 122)**
- **Targeted digital surveillance > Authentication bypass (p. 127)**
- **Targeted digital surveillance > Malware (p. 133)**

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.[79] The sabotage, which took place during the day and involved between 100 and 200 people,[208] 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.[209]

5.6. Repression of the first Jane's Revenge arson

Country: **United States (p. 216)**

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

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

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

Date: **2022 - 2024**
Techniques used:

Forensics > Arson (p. 40)
Forensics > DNA (p. 48)
Forensics > Handwriting analysis (p. 62)
Mass surveillance > Video surveillance (p. 94)
Physical surveillance > Covert (p. 106)

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

In March 2023, a person was arrested[210] and charged with a May 2022 arson attack on the headquarters of an anti-abortion group.[211] 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.[212]

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

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

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

5.7. Repression of the attack on Clarín's headquarters

Country: **Argentina (p. 214)**
Date: **2021 - 2022**
Techniques used:

- **Forensics > Facial recognition (p. 53)**
- **Forensics > Fingerprints (p. 55)**
- **Forensics > Gait recognition (p. 58)**
- **House raid (p. 75)**
- **Mass surveillance > Video surveillance (p. 94)**
- **Network mapping (p. 96)**
- **Open-source intelligence (p. 98)**
- **Service provider collaboration > Mobile network operators (p. 118)**
- **Service provider collaboration > Other (p. 125)**

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.[213]

In a 2022 trial, three of the defendants were sentenced to a three-year suspended prison sentence.[214]

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

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

5.8. Belarusian anarcho-partisans

Country: **Belarus (p. 214)**
Date: **2020 - 2021**
Techniques used:

Mass surveillance > Civilian snitches (p. 87)
Physical violence (p. 110)

In 2020, four people set fire to police buildings and to vehicles in the parking lot of a prosecutor's office.[215] 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.[128] 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.[216]

5.9. Case against Boris

Country: **France (p. 215)**
Date: **2020 - 2021**
Techniques used:

Covert surveillance devices > Location (p. 22)
Covert surveillance devices > Video (p. 25)
Forensics > DNA (p. 46)
ID checks (p. 77)
Interrogation techniques (p. 84)
Mass surveillance > Police files (p. 89)
Mass surveillance > Video surveillance (p. 92)
Physical surveillance > Covert (p. 103)
Service provider collaboration > Mobile network operators (p. 115)

---

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

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

Service provider collaboration > Other (p. 121)
Targeted digital surveillance > IMSI-catcher (p. 130)

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.[22] 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".[217]

5.10. Search for a fugitive

Country: **United States (p. 216)**
Date: **2020 - ?**
Techniques used:

Door knocks (p. 32)
Forensics > DNA (p. 46)
Open-source intelligence (p. 97)
Physical surveillance > Covert (p. 103)
Service provider collaboration > Mobile network operators (p. 116)
Service provider collaboration > Other (p. 121)

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.[7] 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.

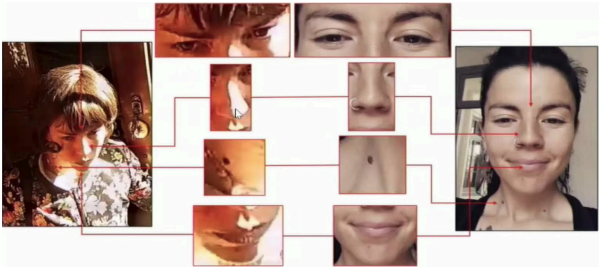
The person was not arrested and is in clandestinity.

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

5.11. 2019-2020 case against Mónica and Francisco

Country: **Chile (p. 214)**
Date: **2019 - 2023**
Techniques used:

Forensics > DNA (p. 46)
Forensics > Facial recognition (p. 52)
Forensics > Handwriting analysis (p. 62)
Mass surveillance > Civilian snitches (p. 86)
Mass surveillance > Video surveillance (p. 92)
Open-source intelligence (p. 97)



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.[45] 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.[218]

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

5.12. Repression against Zündlumpen

Country: **Germany (p. 215)**
Date: **2019 - ?**
Techniques used:

- **Covert house visit (p. 16)**
- **Covert surveillance devices > Audio (p. 19)**
- **Covert surveillance devices > Location (p. 23)**
- **Covert surveillance devices > Video (p. 25)**
- **Detection dogs (p. 30)**
- **Forensics > DNA (p. 46)**
- **Forensics > Linguistics (p. 64)**
- **International cooperation (p. 83)**
- **Mass surveillance > Video surveillance (p. 92)**
- **Network mapping (p. 96)**
- **Open-source intelligence (p. 97)**
- **Physical surveillance > Aerial (p. 100)**
- **Physical surveillance > Covert (p. 103)**
- **Police patrols (p. 112)**
- **Service provider collaboration > Mobile network operators (p. 116)**
- **Service provider collaboration > Other (p. 121)**
- **Targeted digital surveillance > Authentication bypass (p. 127)**
- **Targeted digital surveillance > IMSI-catcher (p. 131)**

In April 2022,[141] October 2022,[219] and February 2025[27] 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.[28]

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.

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

5.13. Repression of the 2019 uprising in Chile

Country: **Chile (p. 214)**
Date: **2019 - 2020**
Techniques used:

Physical surveillance > Aerial (p. 101)
Physical violence (p. 110)

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.[220] 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.[221] Many people were arrested and sentenced to years in prison.

5.14. The three from the park bench

Country: **Germany (p. 215)**
Date: **2019 - ?**
Techniques used:

Mass surveillance > Video surveillance (p. 94)
Physical surveillance > Covert (p. 106)

In 2019, three people were arrested while sitting on a park bench late at night in Hamburg,[108] accused of carrying incendiary devices[222] 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.

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

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

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

In a 2020 trial, the people were sentenced to between 19 and 22 months in prison.[223] The sentences were upheld on appeal in 2022.[224]

5.15. December 8 case

Country: **France (p. 215)**
Date: **2018 - ?**
Techniques used:

- **Biased interpretation of evidence (p. 14)**
- **Covert surveillance devices > Audio (p. 20)**
- **Covert surveillance devices > Location (p. 23)**
- **Covert surveillance devices > Video (p. 26)**
- **Evidence fabrication (p. 33)**
- **Forensics > Trace evidence (p. 70)**
- **House raid (p. 76)**
- **Interrogation techniques (p. 85)**
- **Physical surveillance > Covert (p. 107)**
- **Service provider collaboration > Mobile network operators (p. 118)**
- **Targeted digital surveillance > IMSI-catcher (p. 131)**

On December 8, 2020 several raids took place across the country and nine people were arrested.[225] 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.[226] 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.

---

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

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

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

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

To identify the phone numbers used by some of the defendants, investigators analyzed correlations between different sets of data, obtained through:[20]

- Real-time geolocation of phones, through the **collaboration of mobile network operators (p. 114)**.
- **IMSI-catchers (p. 129)**.
- **Covert location surveillance devices (p. 21)**.
- **Physical surveillance (p. 99)** 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:[227]

- 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. 215)**
Date: **2017 - 2023**
Techniques used:

Covert surveillance devices > Audio (p. 20)
Covert surveillance devices > Location (p. 23)
Covert surveillance devices > Video (p. 25)
Mass surveillance > Civilian snitches (p. 86)
Mass surveillance > Video surveillance (p. 93)

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

Physical surveillance > Covert (p. 104)
Service provider collaboration > Mobile network operators (p. 116)
Service provider collaboration > Other (p. 122)
Targeted digital surveillance > Authentication bypass (p. 128)
Targeted digital surveillance > Malware (p. 133)

In the months preceding October 2023, Italian police tried to find and arrest Stecco, who was on the run.[228] Stecco was accused of helping another person on the run in 2017 and 2018 and of creating fake documents,[229] and also had a cumulative prison sentence of 3 years and 6 months to serve in relation to other cases.[17]

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. 215)**
Date: **2017 - 2022**
Techniques used:

Forensics > Gait recognition (p. 58)
International cooperation (p. 83)

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".[95] 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. 198)**. 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.

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

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

After a trial in 2022, some people were acquitted and some were sentenced to prison, with sentences ranging from 45 days to one year.[230]

5.18. Bure criminal association case

Country: **France (p. 215)**
Date: **2017 - 2025**
Techniques used:

- **Covert surveillance devices > Location (p. 23)**
- **Detection dogs (p. 30)**
- **Forensics > Arson (p. 41)**
- **Forensics > DNA (p. 48)**
- **Forensics > Digital (p. 51)**
- **Forensics > Fingerprints (p. 55)**
- **House raid (p. 74)**
- **International cooperation (p. 83)**
- **Mass surveillance > Police files (p. 90)**
- **Mass surveillance > Video surveillance (p. 94)**
- **Open-source intelligence (p. 98)**
- **Physical surveillance > Covert (p. 106)**
- **Service provider collaboration > Mobile network operators (p. 117)**
- **Service provider collaboration > Other (p. 124)**
- **Targeted digital surveillance > Authentication bypass (p. 128)**
- **Targeted digital surveillance > IMSI-catcher (p. 131)**

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

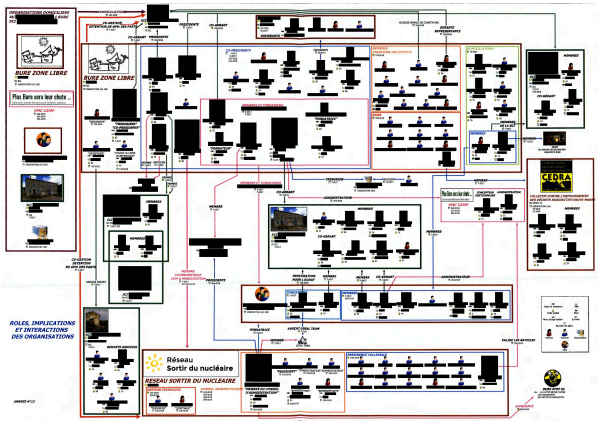


Diagram of the organizations fighting against Cigéo and their members, made by investigators (personal information censored by the No Trace Project).

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.[231] 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).[232]

After a trial in 2021, an appeal in 2023, and another appeal in 2025,[233] everyone was acquitted.

[231] https://bureburebure.info/repression

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

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

5.19. Network

Country: **Russia (p. 216)**
Date: **2017 - 2020**
Technique used:

Physical violence (p. 110)

In late 2017 and early 2018, about ten people were arrested in Penza and Saint Petersburg[127] 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.[234] 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.[235]

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,[236] and two alleged members in Saint Petersburg were sentenced to 5 and a half and 7 years in prison, respectively.[237]

5.20. Panico

Country: **Italy (p. 215)**
Date: **2016 - 2023**
Technique used:

Forensics > DNA (p. 49)

In 2017, house raids took place in Florence and several people were arrested as part of an operation called "Panico".[95] Up to 35 people were charged in

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

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

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

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

this operation.[238] 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[239] and a ruling by the Court of Cassation in 2023,[240] 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. 215)**
Date: **2016 - 2021**
Techniques used:

Evidence fabrication (p. 33)
Forensics > DNA (p. 47)
Mass surveillance > Video surveillance (p. 93)

In 2019, three people were arrested as part of an operation called "Prometeo".[95] 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[241]) for the parcel bombs, although one of them had spent two and a half years in prison before being acquitted.

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

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

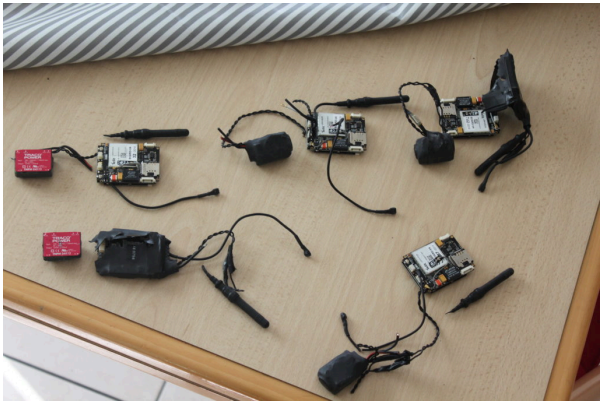
[240] https://lanemesi.noblogs.org/post/2023/07/15/sentenza-di-cassazione-del-processo-panico-14-luglio-2023

[241] https://actforfree.noblogs.org/post/2021/10/06/italy-op-prometeo-beppe-robert-and-nat-acquitted

5.22. Renata

Country: **Italy (p. 215)**
Date: **2016 - 2019**
Techniques used:

Covert surveillance devices > Audio (p. 19)
Forensics > DNA (p. 46)
House raid (p. 73)
Physical violence (p. 110)



Surveillance devices found in a house after the operation.[16]

In February 2019, 50 house raids took place, mainly in Trentino, and seven people were arrested as part of an operation called "Renata".[95] 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. 216)**
Date: **2016 - 2017**
Techniques used:

Interrogation techniques (p. 84)
Physical violence (p. 110)

In 2016, three people were arrested[242] in the parking lot of a police station in Warsaw.[99] They were accused of attempting to set fire to police cars.

The people were detained for 4 months before being released.

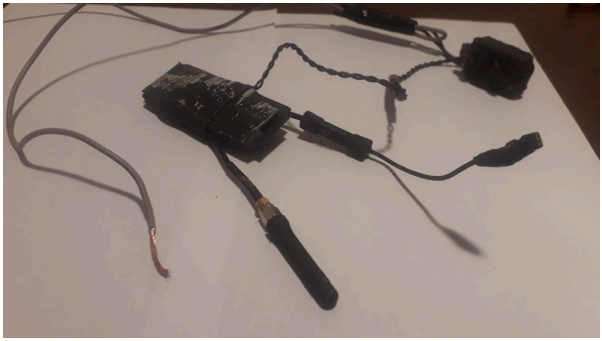
In a 2017 trial, the people were sentenced to 3 months in prison (which they had already served), a fine, and 24 months of community service.

5.24. Scintilla

Country: **Italy (p. 215)**
Date: **2015 - 2023**
Techniques used:

Covert surveillance devices > Audio (p. 20)
Door knocks (p. 32)
Forensics > DNA (p. 48)
Forensics > Gait recognition (p. 58)
International cooperation (p. 83)

[242] https://wawa3.noblogs.org/post/2016/06/21/chronology-eng



Microphones found in a house[19] 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".[95] Some of them were accused of carrying out several arson and explosive attacks on migrant detention centers and other targets between 2015 and 2018.[97] 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.[29] In November 2019, another person, Peppe, was arrested and accused of sending a parcel bomb in 2016 to a company involved in the management of a migrant detention center.[53] 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[243]–2023, several people were sentenced to prison, with sentences ranging from 1 year to 4 years and 2 months.[244]

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

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

5.25. Fenix

Country: **Czech Republic (p. 214)**
Date: **2014 - 2018**
Techniques used:

Detection dogs (p. 30)
Infiltrators (p. 79)
Mass surveillance > Civilian snitches (p. 86)

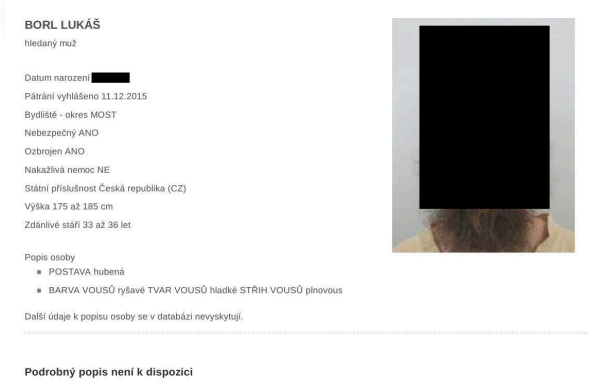


Photo and personal information of Lukáš Borl published on the national police website (date of birth and picture censored by the No Trace Project).[245]

In 2015, house raids took place and several people were charged with crimes as part of an operation called "Fenix".[246] Some of them were accused of the arson of a police car in 2014.[26] 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

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

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

several months.[247]

In a 2017 trial, the people were acquitted. In a 2018 appeal, the acquittals were confirmed.[248]

5.26. 2013 case against Mónica and Francisco

Country: **Spain (p. 216)**
Date: **2013 - 2017**
Techniques used:

Forensics > Facial recognition (p. 53)
House raid (p. 74)
Mass surveillance > Video surveillance (p. 93)

In 2013, Mónica Caballero and Francisco Solar were arrested in Spain, accused of placing an explosive device in a church.[59] 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.[249] In a 2016 appeal, both of their sentences were reduced to 4 years and 6 months.[250] In 2017, Mónica and Francisco were expelled to Chile, their country of origin.[251]

5.27. Case against Revolutionära fronten

Country: **Sweden (p. 216)**
Date: **2013 - 2014**

---

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

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

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

[250]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

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

Techniques used:

Forensics > Digital (p. 51)
House raid (p. 73)
Mass surveillance > Video surveillance (p. 93)
Open-source intelligence (p. 97)
Police patrols (p. 112)
Service provider collaboration > Mobile network operators (p. 116)
Service provider collaboration > Other (p. 122)

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.[7] 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.

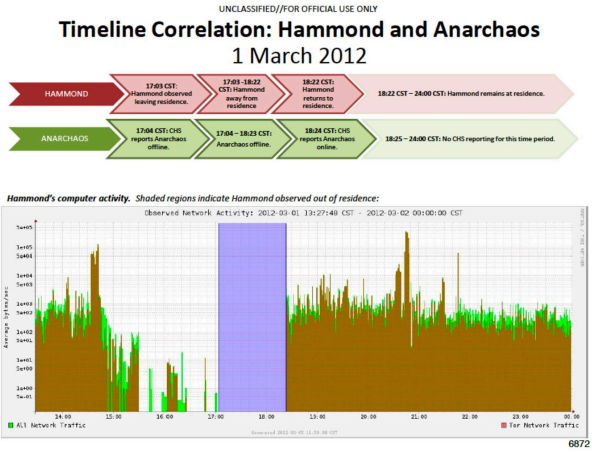
In a 2014 trial:

- 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. 216)**
Date: **2011 - 2013**
Techniques used:

Informants (p. 81)
Mass surveillance > Police files (p. 90)
Physical surveillance > Covert (p. 104)
Targeted digital surveillance > Authentication bypass (p. 128)
Targeted digital surveillance > Network forensics (p. 134)



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.[91]

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.[252]

[252]https://apnews.com/general-news-1632c936e6d74d42aa465878d144aaae

5.29. Nea Filadelphia case

Country: **Greece (p. 215)**
Date: **2011 - 2016**
Techniques used:

Forensics > DNA (p. 49)
Physical surveillance > Covert (p. 107)

In 2013, several people were arrested in Nea Filadelphia, a suburb of Athens.[123] Four of them were accused of carrying out bank robberies[253] in 2011[55] and 2013.[254]

After a trial in 2014, two people were sentenced to 16 years in prison.[255] After another trial in 2014[256] and an appeal in 2016,[257] the other two were sentenced to 9 and 11 years in prison, respectively.

5.30. Case against Amos Mbedzi

Country: **Eswatini (p. 214)**
Date: **2008 - 2012**
Techniques used:

Forensics > DNA (p. 47)
Mass surveillance > Civilian snitches (p. 86)
Physical violence (p. 110)
Service provider collaboration > Mobile network operators (p. 117)

In 2008, Amos Mbedzi took part in an attempt to bomb a bridge in

[253] https://machorka.espivblogs.net/2013/11/06/concerning-the-arrests-of-comrades-in-nea-philadelphia-on-304-athens

[254] https://machorka.espivblogs.net/2016/02/26/appeal-trial-for-the-double-bank-robbery-velvendo-case-greece

[255] https://machorka.espivblogs.net/2014/10/02/announcement-of-sentences-in-the-velvedo-double-robbery-case-11014-athens

[256] https://abcsolidaritycell.espivblogs.net/archives/tag/g-naxakis

[257] https://anarhija.info/library/grecia-l-ultimo-aggiornamento-sul-processo-d-appello-per-rapina-a-pirgetos-con-anarchic-en

Eswatini with an explosive device.[258] 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.[52] 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.[259]

5.31. Mauvaises intentions

Country: **France (p. 215)**
Date: **2006 - 2012**
Techniques used:

- **Forensics > Arson (p. 40)**
- **Forensics > DNA (p. 47)**
- **Network mapping (p. 96)**
- **Physical surveillance > Overt (p. 108)**
- **Service provider collaboration > Mobile network operators (p. 116)**

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.[37] This operation was documented by comrades in a series of zines entitled "Mauvaises intentions".[260]

After a trial in 2012, five people were sentenced to between one and three years in prison.[261]

---

[258] 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

[259] https://peoplesdispatch.org/2022/06/08/south-african-communist-amos-mbedzi-who-fought-apartheid-dies-a-martyr-for-liberation-of-swaziland

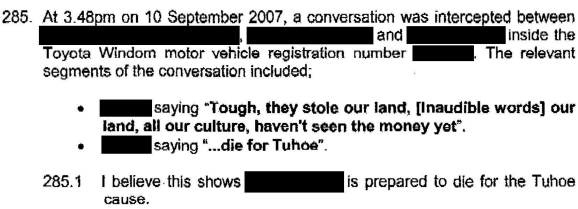
[260] https://notrace.how/resources/#mauvaises-intentions

[261] https://juralib.noblogs.org/2012/06/25/mauvaises-intentions-paris-rendu-du-proces-antiterroriste-de-mai-2012

5.32. Operation 8

Country: **New Zealand (p. 216)**
Date: **2006 - 2012**
Techniques used:

- **Biased interpretation of evidence (p. 13)**
- **Covert surveillance devices > Audio (p. 20)**
- **Covert surveillance devices > Video (p. 26)**
- **Forensics > Gait recognition (p. 58)**
- **House raid (p. 75)**
- **Informants (p. 82)**
- **Network mapping (p. 96)**
- **Open-source intelligence (p. 98)**
- **Physical surveillance > Aerial (p. 101)**
- **Physical surveillance > Covert (p. 107)**
- **Roadblocks (p. 113)**
- **Service provider collaboration > Mobile network operators (p. 117)**
- **Service provider collaboration > Other (p. 124)**



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."[81] 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.[262]

The operation started in 2006 when the police became aware of the "training camps."[6]

In a 2012 trial:

- Two people were sentenced to 2 years and 6 months in prison.[263]
- Two people were sentenced to 9 months of home detention.[264]

5.33. Scripta Manent

Country: **Italy (p. 215)**
Date: **2003 - 2023**
Techniques used:

Forensics > DNA (p. 45)
Forensics > Handwriting analysis (p. 62)
Forensics > Linguistics (p. 64)
House raid (p. 73)
Targeted digital surveillance > Malware (p. 133)

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".[95] 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

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

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

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

Anarchist Federation) since 2003.[265] 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[266] and 2023.[267] 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. 216)**
Date: **2000 - 2008**
Techniques used:

Forensics > Trace evidence (p. 70)
House raid (p. 74)
Physical surveillance > Covert (p. 106)

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.[73] Jeff Luers was later also charged with an attempted arson of trucks at a petroleum products distributor in May 2000.

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

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

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

The June arson charge was based in part on a 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.[268] Craig Marshall was sentenced to 5 and a half years in a plea deal.[269]

5.35. Case against Marius Mason

Country: **United States (p. 216)**
Date: **1999 - 2010**
Technique used:

Informants (p. 81)

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)[88] from 1999 to 2003,[270] 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.

5.36. Case against Direct Action

Country: **Canada (p. 214)**
Date: **1982 - 1986**
Techniques used:

Covert house visit (p. 16)
Covert surveillance devices > Audio (p. 20)

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

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

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

Forensics > Linguistics (p. 64)
House raid (p. 75)
Mass surveillance > Civilian snitches (p. 87)
Physical surveillance > Aerial (p. 101)
Physical surveillance > Covert (p. 107)

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.[11] 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,[82] 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.

6. Countries

6.1. Argentina

Repressive operation:

Repression of the attack on Clarín's headquarters (p. 187)

6.2. Belarus

Repressive operation:

Belarusian anarcho-partisans (p. 188)

6.3. Canada

Repressive operation:

Case against Direct Action (p. 212)

6.4. Chile

Repressive operations:

2019-2020 case against Mónica and Francisco (p. 190)
Repression of the 2019 uprising in Chile (p. 192)

6.5. Czech Republic

Repressive operation:

Fenix (p. 203)

6.6. Eswatini

Repressive operation:

6.7. France

Repressive operations:

6.8. Germany

Repressive operations:

6.9. Greece

Repressive operation:

6.10. Italy

Repressive operations:

6.11. New Zealand

Repressive operation:
Operation 8 (p. 209)

6.12. Poland

Repressive operation:
Warsaw 3 (p. 201)

6.13. Russia

Repressive operations:
Network (p. 198)
Case against Ruslan Siddiqi (p. 184)

6.14. Spain

Repressive operation:
2013 case against Mónica and Francisco (p. 204)

6.15. Sweden

Repressive operation:
Case against Revolutionära fronten (p. 204)

6.16. United States

Repressive operations:
Case against Marius Mason (p. 212)
Case against Jeff Luers (p. 211)
2011-2013 case against Jeremy Hammond (p. 205)
Search for a fugitive (p. 189)

Repression of the first Jane's Revenge arson (p. 185)
Case against Peppy and Krystal (p. 183)

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*.[271]

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

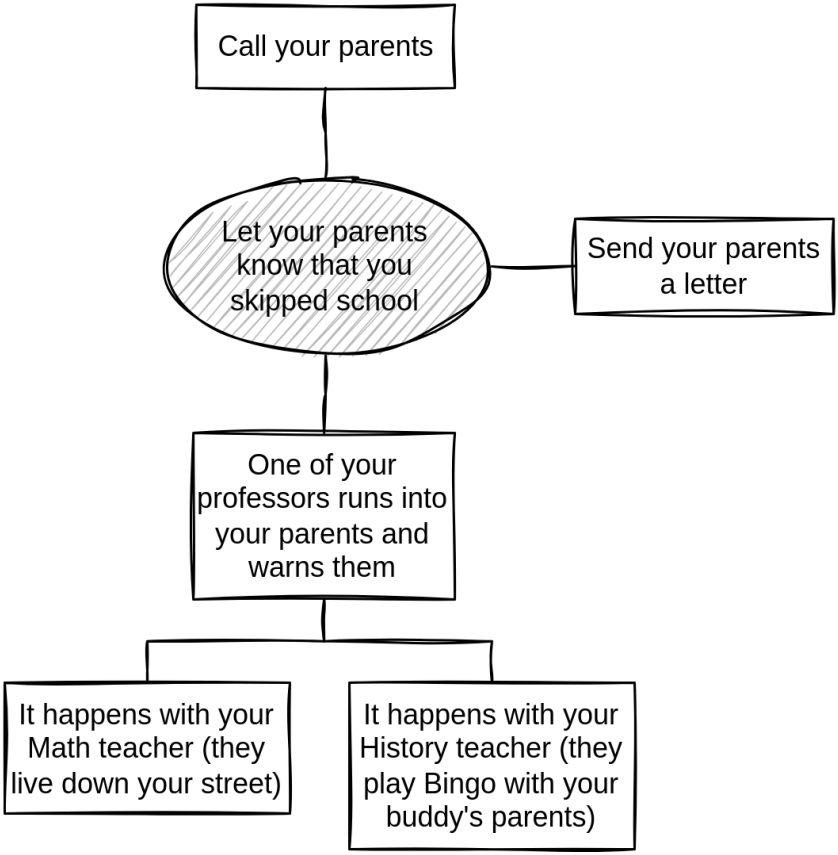
Let's start with a simple example before we consider a real one. You're a kid in school, and you and your buddy want to skip a day of school, but you don't want your parents to know. The adversary is the school system.

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

[271] 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

—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.

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. 169)**.

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*.

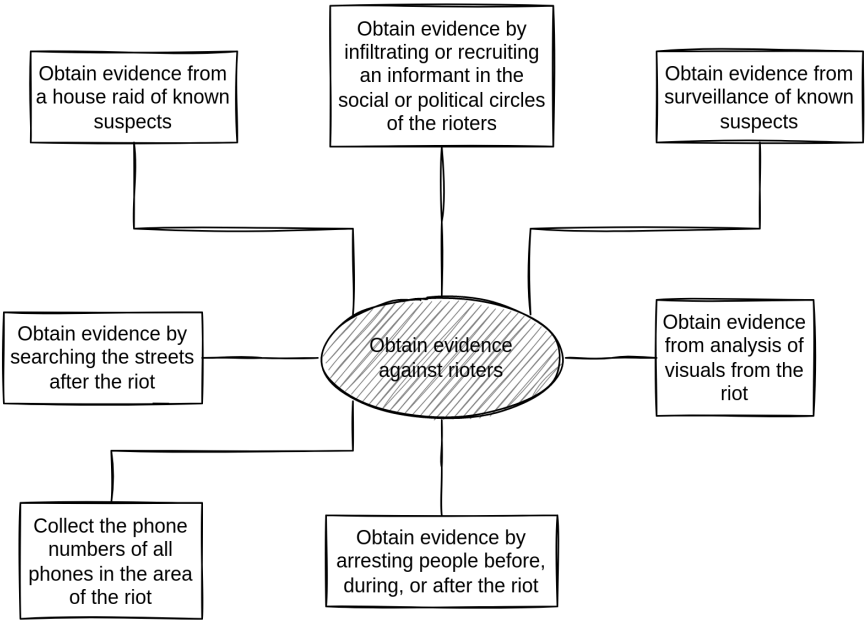
7.2.1. Draw the attack tree

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.[272] You begin with the root node (2).

[272] 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).

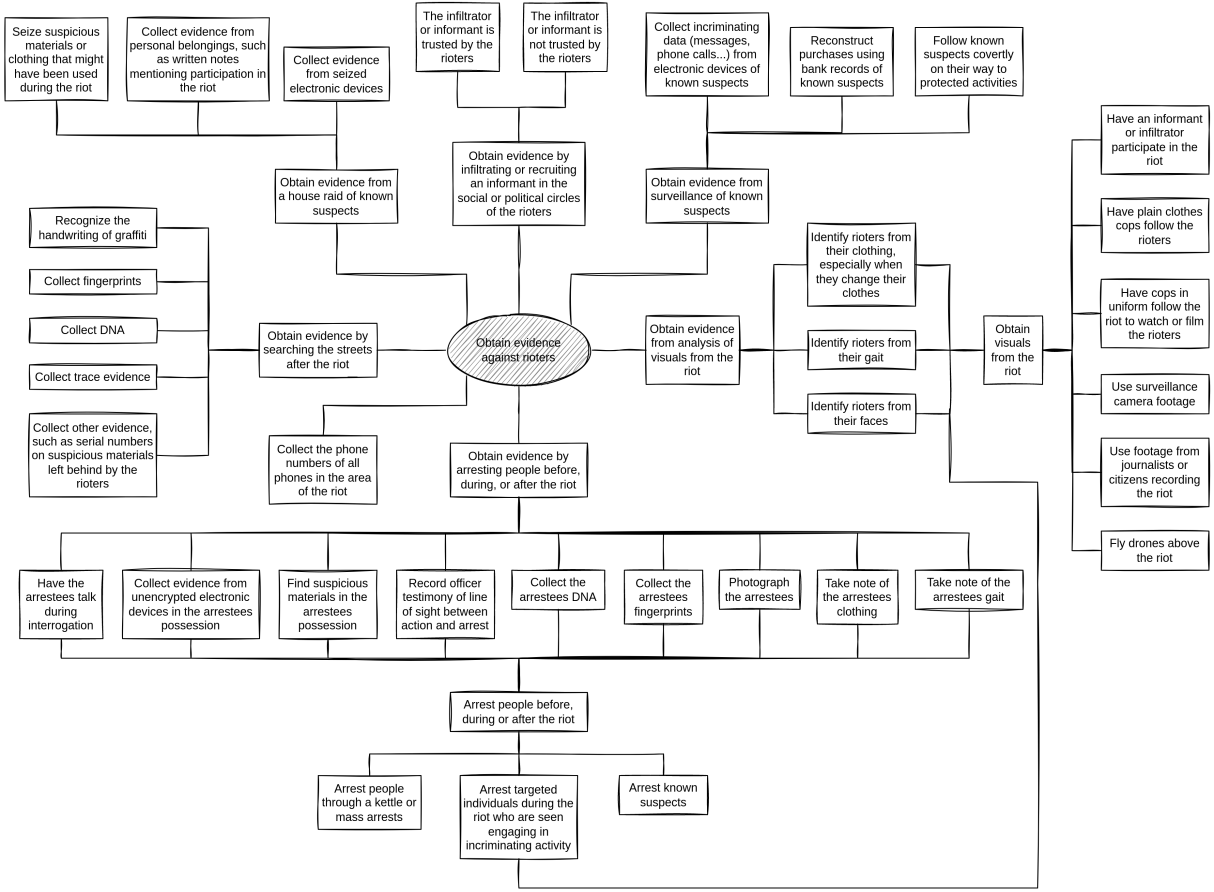
(2) “Riot” attack tree (root node).

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).

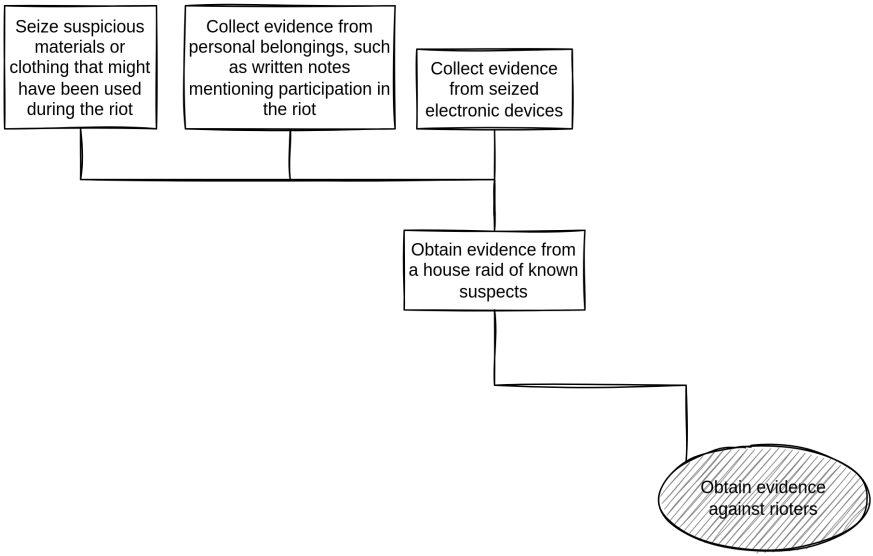
You use the Threat Library to help grow the tree—reading about techniques helps you better understand all the options available to your adversary. Creating attack trees requires a certain mindset and takes practice. The tree is complete when no more nodes are needed to complete an attack, and every attack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



(4) “Riot” attack tree (complete).

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 (p. 72)**.
- "Collect evidence from seized electronic devices" matches **Targeted digital surveillance: Physical access (p. 135)** because they would access your electronic devices, and **Targeted digital surveillance: Authentication bypass (p. 126)**, 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. 229 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. 172)**, **Preparing for house raids (p. 171)** and **Stash spot or safe house (p. 174)**. You don't want to implement **Clandestinity (p. 150)** because you decide against going down that road.
- For the two "Targeted digital surveillance" techniques, **Digital best practices (p. 152)** is the only mitigation that makes sense in your context.

You update the table (7).

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

(7) Beginning of the table, with mitigations.

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[57] (remember to follow **digital best practices (p. 152)**). 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. 169)**, 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.

7.3. Assessing risk

Risk is the combined measure of a technique's impact and likelihood. If a technique would have a high impact, but is very unlikely to be used, it might be considered low risk. If a technique would have a medium impact, but is likely to be used, it might be considered high risk. If you consider the risk of a technique to be high, it means that you should apply mitigations for it more thoroughly.

For example, in most contexts, if you are planning to commit arson, the **Forensics: DNA (p. 42)** 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. 160)** 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. 182)** 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[273] 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:

- 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. 232)** for more information.

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

8. Contribute to the Threat Library

8.1. Contact

Is there a **technique (p. 12)**, **mitigation (p. 137)**, or **repressive operation (p. 182)** 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[274])

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.[275]

[274] https://notrace.how/notrace.asc

[275] https://notrace.how/translations.html

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.

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.