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

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

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

Threat Library

Part 3/3

Mitigations, Repressive operations, Countries

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

Original publication by the No Trace Project

notrace.how/threat-library

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

April 11, 2024

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

Contents

8. Contribute to the Threat Library

8.1. Contact

Is there a **technique (#2)**, **mitigation (p. 5)**, or **repressive operation (p. 49)** 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)

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 or North America, but we welcome contributions from these regions as well.

8.3. Translations

To coordinate translations across the No Trace Project, we use the Weblate collaborative localization platform. To translate the Threat Library into a new language, or to improve an existing translation, register an account on the Weblate instance used by the No Trace Project[112] (you will need an email address) and follow the instructions[113]. All languages are welcome.

[112] https://weblate.anarchyplanet.org
[113] https://weblate.anarchyplanet.org/projects/ntp/#information

7.6. Italy

Repressive operations:

Scripta Manent (p. 62)
Scintilla (p. 59)
Panico (p. 57)
Prometeo (p. 57)
Renata (p. 58)
Bialystok (p. 55)

7.7. Russia

Repressive operations:

Network (p. 56)

7.8. Spain

Repressive operations:

2013 case against Mónica and Francisco (p. 60)

7.9. United States

Repressive operations:

Case against Marius Mason (p. 64)
Case against Jeff Luers (p. 64)
Repression of the first Jane's Revenge arson (p. 50)

5. Mitigations

5.1. Anonymous dress

Techniques addressed by this mitigation:

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

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

7. Countries

7.1. Belarus

Repressive operations:

Belarusian anarcho-partisans (p. 51)

7.2. Chile

Repressive operations:

2019-2020 case against Mónica and Francisco (p. 52)
Repression of the 2019 uprising in Chile (p. 54)

7.3. France

Repressive operations:

Mauvaises intentions (p. 62)
Case against Boris (p. 52)
Repression of Lafarge factory sabotage (p. 49)

7.4. Germany

Repressive operations:

Repression against Zündlumpen (p. 53)
The three from the park bench (p. 55)
Berlin 2023 railway conspiracy case (p. 49)

7.5. Greece

Repressive operations:

Nea Filadelphia case (p. 61)

(ELF) and the Animal Liberation Front (ALF)[110] from 1999 to 2003[111], 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.

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

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

To hide your body features, you can:

- To hide your face: wear a mask that adequately covers your face, including your eyebrows and up to the top of your nose.
- To hide the rest of your body: wear a shirt with long sleeves, gloves, pants with long legs, and high socks.
- To hide your skin color: make sure no skin is visible, including around your eyes, at the junction of your shirt and gloves, and at the junction of your pants and socks.
- To hide your body shape and gait: wear baggy clothing (you can also conceal your gait with **biometric concealment (p. 14)**).

Ensure that clothing cannot be used to identify you

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

1. **Anonymously purchase (p. 8)** two sets of clothing specifically for the action, "civilian clothing" and "action clothing":
    - Civilian clothing is clothing that is normal to wear in public. It can include items that hide your body features as long as it isn't suspicious (e.g., a hat, a "Covid" mask).
    - Action clothing is clothing that adequately hides your body features, as described above.
2. Far away from the action site, change from your regular clothing into the civilian clothing, in a suitable place where there are no surveillance cameras or witnesses.
3. Close to the action site, change into the action clothing (in a suitable place).
4. Perform the action.
5. Close to the action site, change back into the civilian clothing (in a suitable place).
6. Far away from the action site, change back into your regular clothing (in a suitable place).
7. Dispose of the civilian clothing and the action clothing safely.

The "black bloc"

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

5.2. Anonymous phones

Techniques addressed by this mitigation:

Network mapping (#2)
Service provider collaboration (#2)

An anonymous phone is a phone that is not tied to your identity. A burner phone is a type of 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 number needs to be stable in the long term, you should always prefer burner phones.

To setup and use an anonymous phone:

- **Anonymously purchase (p. 8)** 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 **mobile network operator collaboration (#2)**.

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 (#2)**—especially if all members of a scene or network use them—but you should not use them for sensitive projects or actions.

See also

6.20. Case against Jeff Luers

Countries: **United States (p. 67)**
Date: 2000 - 2008
Techniques used:

Forensics > Trace evidence (#2)
House raid (#2)
Physical surveillance > Mobile (#2)

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[107]. Jeff Luers was later also charged with an attempted arson of trucks at a petroleum products distributor in May 2000.

The June arson charge was based in part on a mobile 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[108]. Craig Marshall was sentenced to 5 and a half years in a plea deal[109].

6.21. Case against Marius Mason

Countries: **United States (p. 67)**
Date: 1999 - 2010
Techniques used:

Informants (#2)

In 2008, Marius Mason was arrested and charged with several acts of arson and other vandalism claimed by the Earth Liberation Front

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

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

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

Forensics > DNA (#2)
Forensics > Handwriting analysis (#2)
Forensics > Linguistics (#2)
House raid (#2)
Targeted digital surveillance > Malware (#2)

In 2016, 32 house raids took place in different regions of Italy and several anarchist comrades were arrested as part of an operation called "Scripta Manent"[72]. Up to 22 comrades were under investigation in this operation. They were accused of forming or participating in an *associazione sovversiva con finalità di terrorismo* (criminal association with the aim of terrorism), referring to attacks claimed by the *Federazione Anarchica Informale* (FAI, Informal Anarchist Federation) since 2003[104]. 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[105] and 2023[106]. The final verdict is:

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

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

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

[106] 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

See Burner Phone Best Practices[1] for more information on burner phones.

5.3. Anonymous purchases

Techniques addressed by this mitigation:
Forensics > Arson (#2)
Forensics > Ballistics (#2)
Mass surveillance > Video surveillance (#2)
Service provider collaboration (#2)

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

You should anonymously purchase any materials you plan to use for a sensitive project or action. This way:

- If an adversary finds the materials at the action site (e.g., an incendiary device with a delay that failed) or traces of the materials (e.g., traces of accelerant discovered by **arson forensics (#2)**) and discovers where the materials were purchased, they will not discover your identity.
- If an adversary obtains your bank records through the **collaboration of your bank (#2)**, 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. 47)**), and do not bring a phone.

[1] https://notrace.how/resources/#burner-phone-best-practices

- Conduct **anti-surveillance (p. 9)** before going to the store.
- Use some level of **anonymous dress (p. 5)** to be less recognizable —a Covid mask, a hat, dedicated clothing.
- Pay in cash.
- Make sure your interaction with the cashier is not memorable.
- If you have to purchase several items, you can make the purchases in different stores, in different locations, at different times. This is especially important if you purchase items that would be suspicious to purchase together.

Digital anonymous purchases

You can make digital anonymous purchases with cryptocurrencies. You should either acquire the cryptocurrencies anonymously, or sufficiently launder them before using them, which can be a hassle, but is possible with cryptocurrencies like Monero using Tails[2].

See also

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

5.4. Anti-surveillance

Techniques addressed by this mitigation:
Physical surveillance > Aerial (#2)
Physical surveillance > Mobile (#2)

Anti-surveillance is the practice of taking active measures to evade ("shake off") a **mobile physical surveillance effort (#2)**.

When to conduct anti-surveillance

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

[2]https://anonymousplanet.org/guide.html#your-cryptocurrencies-transactions
[3]https://notrace.how/resources/#prisma

After a trial in 2014, two comrades were sentenced to 16 years in prison[98]. After another trial in 2014[99] and an appeal in 2016[100], the other two were sentenced to 9 and 11 years in prison, respectively.

6.18. Mauvaises intentions

Countries: **France (p. 66)**
Date: 2006 - 2012
Techniques used:
Forensics > DNA (#2)
Network mapping (#2)
Physical surveillance > Overt (#2)
Service provider collaboration (#2)

In 2008, six comrades 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[101]. This operation was documented by comrades in a series of zines entitled "Mauvaises intentions[102]".

After a trial in 2012, five comrades were sentenced to between one and three years in prison[103].

6.19. Scripta Manent

Countries: **Italy (p. 67)**
Date: 2003 - 2023
Techniques used:

[98]https://machorka.espivblogs.net/2014/10/02/announcement-of-sentences-in-the-velvedo-double-robbery-case-11014-athens
[99]https://abcsolidaritycell.espivblogs.net/archives/tag/g-naxakis
[100]https://anarhija.info/library/grecia-l-ultimo-aggiornamento-sul-processo-d-appello-per-rapina-a-pirgetos-con-anarchic-en
[101]https://infokiosques.net/spip.php?article597
[102]https://notrace.how/resources/#mauvaises-intentions
[103]https://juralib.noblogs.org/2012/06/25/mauvaises-intentions-paris-rendu-du-proces-antiterroriste-de-mai-2012

House raid (#2)
Mass surveillance > Video surveillance (#2)

In 2013, anarchists Mónica Caballero and Francisco Solar were arrested in Spain, accused of placing an explosive device in a church[90]. 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[91]. In a 2016 appeal, both of their sentences were reduced to 4 years and 6 months[92]. In 2017, Mónica and Francisco were expelled to Chile, their country of origin[93].

6.17. Nea Filadelphia case

Countries: **Greece (p. 66)**
Date: 2011 - 2016
Techniques used:
Forensics > DNA (#2)
Physical surveillance > Mobile (#2)

In 2013, several comrades were arrested in Nea Filadelphia, a suburb of Athens[94]. Four of them were accused of carrying out bank robberies[95] in 2011[96] and 2013[97].

[90]https://notrace.how/documentation/monica-and-francisco-2013-case-file.pdf
[91]https://alasbarricadas.org/noticias/node/36054
[92]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
[93]https://es-contrainfo.espiv.net/2017/03/10/estado-espanol-comunicado-de-lxs-companerxs-anarquistas-monica-caballero-y-francisco-solar
[94]https://web.archive.org/web/20201027031238/http://actforfree.nostate.net/?p=15472
[95]https://machorka.espivblogs.net/2013/11/06/concerning-the-arrests-of-comrades-in-nea-philadelphia-on-304-athens
[96]https://abcsolidaritycell.espivblogs.net/archives/130
[97]https://machorka.espivblogs.net/2016/02/26/appeal-trial-for-the-double-bank-robbery-velvendo-case-greece

- **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 effort 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 effort 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 effort. 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 effort is planning to take immediate violent action against you, conducting anti-surveillance would reveal to the surveillance effort that you know they are following you, which could push the adversary to adapt and be more discreet, which you want to avoid.

A core principle

A core principle of anti-surveillance is that, usually, a surveillance effort 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 effort, 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 effort needs to stay far away from you to avoid detection, to a less open area, where the surveillance effort 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 effort 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.

In February 2019, the *Asilo Occupato* squat in Turin was evicted and six anarchist comrades were arrested—a seventh comrade, Carla, went on the run—as part of an operation called "Scintilla"[72]. Some of them were accused of carrying out several arson and explosive attacks on migrant detention centers and other targets between 2015 and 2018[85]. 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 comrade, Boba, was arrested and accused of setting fire to a prison building with a nautical flare during a gathering in front of the prison where the other comrades were detained[86]. In November 2019, another comrade, Peppe, was arrested and accused of sending a parcel bomb in 2016 to a company involved in the management of a migrant detention center[87]. 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[88]–2023, several comrades were sentenced to prison, with sentences ranging from 1 year to 4 years and 2 months[89].

6.16. 2013 case against Mónica and Francisco

Countries: **Spain (p. 67)**
Date: 2013 - 2017
Techniques used:
Forensics > Facial recognition (#2)

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

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

[87] https://roundrobin.info/2019/12/verona-una-perquisizione-e-un-arresto

[88] https://roundrobin.info/2021/10/op-scintilla-inizio-del-processo-e-volantino

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

In February 2019, 50 house raids took place, mainly in Trentino, and seven anarchist comrades were arrested as part of an operation called "Renata"[72]. More comrades were arrested in May 2019. The arrested comrades 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 comrades were also accused of forging documents.

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

6.15. Scintilla

Countries: **Italy (p. 67)**
Date: 2015 - 2023
Techniques used:

Covert surveillance devices > Audio (#2)
Door knocks (#2)
Forensics > DNA (#2)
Forensics > Gait recognition (#2)
International cooperation (#2)

Microphones found in a house[84] that were used to surveil the accused comrades.

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

See also

See the physical surveillance topic[4].

5.5. Attack

Techniques addressed by this mitigation:

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

Many repressive techniques are effectively mitigated by a simple maxim: the best defense is a strong 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[5] and P25[6] antennas, and police operations depend on the integrity of their vehicle fleets, stations, and individual officers' feelings of safety. The possibilities for attack are limited only by one's imagination.

[4]https://notrace.how/resources/#topic=physical-surveillance
[5]https://en.wikipedia.org/wiki/Terrestrial_Trunked_Radio#Usage
[6]https://en.wikipedia.org/wiki/Project_25

5.6. Avoiding self-incrimination

Techniques addressed by this mitigation:

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

An enormous number of convictions are based on self-incrimination—behaviour that essentially amounts to snitching on yourself.

If you are arrested, don't talk to the police. Any communication beyond the legal requirements (often name, date and place of birth) should be considered self-incrimination, and depending on your context you may be released without divulging even this information.

Don't 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 communications and devices are hostile terrain. Don't let anything incriminating go through your phone as a text message, photo, etc.—regardless of **encryption (p. 28)**. Social media is a treasure trove for State adversaries: don't use social media, or at least don't post anything incriminating on social media. Taking videos or photos during riots incriminates people and should be considered a form of snitching[7]: don't take videos or photos during riots.

Depending on your context, refusing to provide identification and biometric information (face photograph, fingerprints, DNA) upon arrest by a State adversary may be a viable strategy.

See the related mitigation **Need to know principle (p. 34)**.

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

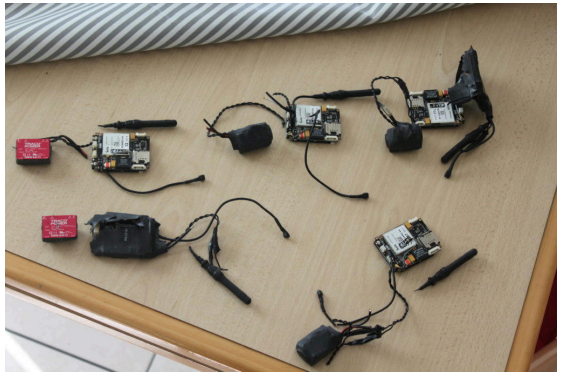
In 2019, three anarchist comrades were arrested as part of an operation called "Prometeo"[72]. They were accused of sending parcel bombs to prosecutors and a director of the prison administration in 2017. One of the comrades was also accused of carrying out an arson attack on an ATM in 2016.

In 2021, the comrade accused of the ATM arson was sentenced to 5 years in prison, while all the comrades were acquitted (for lack of evidence[82]) for the parcel bombs, although one of them had spent two and a half years in prison before being acquitted.

6.14. Renata

Countries: **Italy (p. 67)**
Date: 2016 - 2019
Techniques used:

Covert surveillance devices > Audio (#2)
Extra-legal violence (#2)
Forensics > DNA (#2)
House raid (#2)



Surveillance devices found in a house after the operation[83].

[82] https://actforfree.noblogs.org/post/2021/10/06/italy-op-prometeo-beppe-robert-and-nat-acquitted
[83] https://notrace.how/earsandeyes/#trento-2019-03

6 to 18 years[77], and two alleged members in Saint Petersburg were sentenced to 5 and a half and 7 years in prison, respectively[78].

6.12. Panico

Countries: **Italy (p. 67)**
Date: 2016 - 2023
Techniques used:
Forensics > DNA (#2)

In 2017, house raids took place in Florence and several anarchist comrades were arrested as part of an operation called "Panico"[72]. Up to 35 comrades were charged in this operation[79]. Some comrades were accused of carrying out an explosive attack on a fascist bookshop in 2017 and an arson attack on a police station in 2016. Other comrades were accused of various other actions.

After a trial in 2019, an appeal in 2021[80] and a ruling by the Court of Cassation in 2023[81], two comrades were sentenced to 8 years in prison, while others received sentences ranging from a few months to three and a half years.

6.13. Prometeo

Countries: **Italy (p. 67)**
Date: 2016 - 2021
Techniques used:
Forensics > DNA (#2)
Mass surveillance > Video surveillance (#2)
Service provider collaboration (#2)

[77] https://therussianreader.com/2020/02/10/network-penza-sentences
[78] https://anarchistsworldwide.noblogs.org/post/2020/06/23/saint-petersburg-russia-we-can-dance-if-we-want-to-sentencing-of-the-network-case-defendants
[79] https://insuscettibilediravvedimento.noblogs.org/post/2019/07/18/it-en-italia-richieste-di-condanna-al-processo-per-loperazione-panico
[80] https://ilrovescio.info/2021/05/05/sentenza-dappello-processo-panico
[81] https://lanemesi.noblogs.org/post/2023/07/15/sentenza-di-cassazione-del-processo-panico-14-luglio-2023

5.7. Background checks

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

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

Performing a background check on someone may involve:

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

We recommend two different approaches to background checks:

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

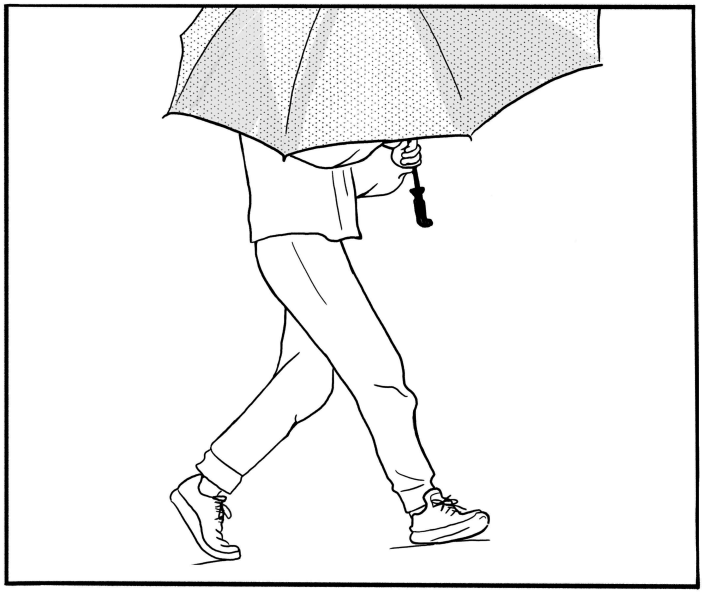
For more information on background checks, see Confidence, Courage, Connection, Trust[8].

5.8. Biometric concealment

Techniques addressed by this mitigation:
Forensics > Facial recognition (#2)
Forensics > Gait recognition (#2)
Forensics > Handwriting analysis (#2)

[8] https://notrace.how/resources/#confidence-courage-connection-trust

Forensics > Linguistics (#2)
Mass surveillance > Video surveillance (#2)



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[9] and the chapter "Traces" in Prisma[3].

5.9. Bug search

Techniques addressed by this mitigation:

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

A bug search is the active process of trying to detect the presence of **covert surveillance devices (#2)** in a building, vehicle, or outdoor

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

operation (p. 57). Two of them were accused of carrying out an explosive attack on a police station in 2017 and an arson attack on cars linked to ENI (an Italian multinational oil and gas company) in 2019, respectively.

After a trial in 2022, some comrades were acquitted and some were sentenced to prison, with sentences ranging from 45 days to one year[73].

6.11. Network

Countries: **Russia (p. 67)**
Date: 2017 - 2020
Techniques used:

Extra-legal violence (#2)

In late 2017 and early 2018, about ten anarchists and antifascists were arrested in Penza and Saint Petersburg[74] and accused of being part of an underground organization called "Network" that was planning terrorist attacks in anticipation of the 2018 Russian presidential elections and the FIFA World Cup[75]. 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).

According to the case files and other information, the initial arrests that launched the investigation were made because most of the defendants from Penza were involved in the drug business[76].

After two trials in 2020, seven alleged members of the "Network" organization in Penza were sentenced to prison terms ranging from

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

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

[75] https://www.amnesty.org/en/wp-content/uploads/2021/05/EUR4696252018ENGLISH.pdf

[76] https://web.archive.org/web/20210724130151/https://a2day.net/the-dark-side-of-the-network-case

6.9. The three from the park bench

Countries: **Germany (p. 66)**
Date: 2019 - ?
Techniques used:
Mass surveillance > Video surveillance (#2)
Physical surveillance > Mobile (#2)

In 2019, three comrades were arrested while sitting on a park bench late at night in Hamburg[68], accused of carrying incendiary devices[69] and planning to burn down a specific building whose address was written on a piece of paper found on them. Two of the arrested comrades had been followed by cops for several hours before their arrest.

In a 2020 trial, the comrades were sentenced to between 19 and 22 months in prison[70]. The sentences were upheld on appeal in 2022[71].

6.10. Bialystok

Countries: **Italy (p. 67)**
Date: 2017 - 2022
Techniques used:
Forensics > Gait recognition (#2)
International cooperation (#2)

In June 2020, house raids took place in the *Bencivenga Occupato* squat in Rome and other places, and seven anarchist comrades were arrested in Italy, Spain and France as part of an operation called "Bialystok"[72]. They were accused of participating in an *associazione sovversiva* (criminal association) and of various minor offenses related to initiatives in solidarity with comrades accused in the **Panico**

[68] https://notrace.how/resources/#observationen-und-andere-argernisse
[69] https://parkbanksolidarity.blackblogs.org/509
[70] https://parkbanksolidarity.blackblogs.org/end-of-the-trial-two-imprisoned-comrades-on-the-streets-again
[71] 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
[72] https://malacoda.noblogs.org/anarchici-imprigionati

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. 36)**.

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. 47)**, 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. 43)**.

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[10] for a database of cases of covert surveillance devices used against anarchists and other rebels.

5.10. Careful action planning

Techniques addressed by this mitigation:

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

When planning an action, careful action planning is the sensible development of the action plan. It follows **reconnaissance (p. 40)**.

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

Forensics > DNA (#2)
Service provider collaboration (#2)
Targeted digital surveillance > Authentication bypass (#2)

In April 2022[64] and October 2022[65], several apartments and basements, a print shop, and a library were raided by police as part of an investigation into the alleged editors of the German anarchist newspaper *Zündlumpen*, published from 2019 to 2021.

During the April 2022 raid on the print shop, 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.

6.8. Repression of the 2019 uprising in Chile

Countries: **Chile (p. 66)**
Date: 2019 - 2020
Techniques used:

Extra-legal violence (#2)
Physical surveillance > Aerial (#2)

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[66]. 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[67]. Many people were arrested and sentenced to years in prison.

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

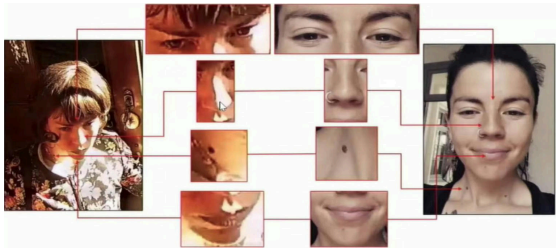
[65]https://de.indymedia.org/node/234616

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

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

Techniques used:

Forensics > DNA (#2)
Forensics > Facial recognition (#2)
Forensics > Handwriting analysis (#2)
Mass surveillance > Civilian snitches (#2)
Mass surveillance > Video surveillance (#2)
Open-source intelligence (#2)



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, anarchists 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[62]. Both have been charged with attempted murder.

In a trial in 2023, Francisco Solar was sentenced to 86 years in prison and Mónica Caballero to 12 years[63].

6.7. Repression against Zündlumpen

Countries: **Germany (p. 66)**
Date: 2019 - ?
Techniques used:

[62] https://notrace.how/resources/#uber-orwell-und-der-fall-von-monica-und-francisco

[63] https://informativoanarquista.noblogs.org/post/2023/12/08/chile-condenas-contra-lxs-companerxs-monica-caballero-y-francisco-solar

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. 9)** prior to the action meeting point?

5.11. Clandestinity

Techniques addressed by this mitigation:

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

Clandestinity is the process of breaking away from your established identity and begin a new life with a **fake identity (p. 29)**.

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[11].

5.12. Compartmentalization

Techniques addressed by this mitigation:

Network mapping (#2)
Targeted digital surveillance > Malware (#2)
Targeted digital surveillance > Network forensics (#2)

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

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 know that they belong to the same person.
- Using different Tails[12] USB sticks or Qubes OS[13] virtual machines for different digital identities. This way, if an adversary compromises one stick or virtual machine with **malware (#2)**, 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. 34)** 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. 9)** measures when traveling

[12]https://tails.boum.org
[13]https://www.qubes-os.org

6.5. Case against Boris

Countries: **France (p. 66)**
Date: 2020 - 2021
Techniques used:

Covert surveillance devices > Location (#2)
Covert surveillance devices > Video (#2)
Forensics > DNA (#2)
ID checks (#2)
Interrogation techniques (#2)
Mass surveillance > Police files (#2)
Mass surveillance > Video surveillance (#2)
Physical surveillance > Mobile (#2)
Service provider collaboration (#2)
Targeted digital surveillance > IMSI-catcher (#2)

In 2020, Boris, an anarchist from France, 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[60]. 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 to four years for the sabotage on Mount Poupet, with two to be served in prison and two on probation. After his trial, he publicly claimed responsibility for the sabotage in a text entitled "Why I burned the two antennas on Mount Poupet"[61].

6.6. 2019-2020 case against Mónica and Francisco

Countries: **Chile (p. 66)**
Date: 2019 - 2023

[60]https://rupture.noblogs.org/post/2023/10/04/no-bars
[61]https://anarchistnews.org/content/why-i-burned-2-antennas

In March 2023, a comrade was arrested[54] and charged with a May 2022 arson attack on the headquarters of an anti-abortion group[55]. 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 comrade was sentenced to 7 and a half years in prison[56].

6.4. Belarusian anarcho-partisans

Countries: **Belarus (p. 66)**
Date: 2020 - 2021
Techniques used:
Extra-legal violence (#2)
Mass surveillance > Civilian snitches (#2)

In 2020, four anarchists set fire to police buildings and vehicles in the parking lot of a prosecutor's office[57]. Soon after, they were arrested by border guards while trying to cross the Belarusian-Ukrainian border.

In the first days of their detention, the anarchists were tortured[58]. 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[59].

[54]https://www.washingtontimes.com/news/2023/mar/28/hridindu-sankar-roychowdhury-arrested-charged-fire
[55]https://janesrevenge.noblogs.org/2022/05/08/first-communique
[56]https://madison.com/news/local/crime-courts/hridindu-roychowdhury-crime-abortion-madison-wisconsin/article_af329b98-f752-11ee-a846-632571f96ea2.html
[57]https://pramen.io/en/2020/11/open-letter-in-support-of-belarus-anarchist-revolutionaries
[58]https://pramen.io/en/2021/12/blood-on-your-hands-regarding-information-about-torture-of-anarcho-partisans
[59]https://abc-belarus.org/en/2021/12/22/18-to-20-years-imprisonment-for-belarusian-anarcho-partisans

as part of a specific project, but not make the same effort for another, less sensitive project.

5.13. Computer and mobile forensics

Techniques addressed by this mitigation:
Targeted digital surveillance > Malware (#2)
Targeted digital surveillance > Physical access (#2)

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

See also:

- The Device Integrity[14] page on Privacy Guides.
- Practical Linux Forensics[15] for a comprehensive introduction to the skill set on Linux, the platform most relevant to anarchists and other rebels.

5.14. DNA minimization protocols

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

[14]https://privacyguides.org/en/device-integrity
[15]https://notrace.how/resources/#practical-linux-forensics

DNA minimization protocols allow you to manipulate objects while minimizing the amount of **DNA (#2)** you leave on them. Some protocols focus on never leaving DNA traces on an object in the first place. Other protocols focus on removing DNA traces from an object by chemically destroying DNA molecules.

DNA minimization protocols may involve:

- Purchasing an object in individual plastic packaging so that you don't risk leaving DNA on it until you open the packaging.
- Manipulating an object while wearing a new pair of non-permeable gloves (e.g. dish washing gloves) so that there are no DNA traces on the outside of the gloves that could be transferred to the object.
- 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.

which took place during the day and involved between 100 and 200 activists[52], 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[53].

6.3. Repression of the first Jane's Revenge arson

Countries: **United States (p. 67)**
Date: 2022 - ?
Techniques used:

Forensics > DNA (#2)
Forensics > Handwriting analysis (#2)
Mass surveillance > Video surveillance (#2)
Physical surveillance > Mobile (#2)

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

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

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

6. Repressive operations

6.1. Berlin 2023 railway conspiracy case

Countries: **Germany (p. 66)**
Date: 2023 - ?
Techniques used:

Physical surveillance > Aerial (#2)

In February 2023, a few minutes after midnight, during a routine surveillance flight, the helicopter of the German federal police identified two comrades on railroad tracks near Berlin[50]. Three police cars were dispatched to the location and the comrades were arrested on suspicion of attempted arson against the railway infrastructure.

6.2. Repression of Lafarge factory sabotage

Countries: **France (p. 66)**
Date: 2022 - ?
Techniques used:

Forensics > DNA (#2)
House raid (#2)
Mass surveillance > Video surveillance (#2)
Open-source intelligence (#2)
Service provider collaboration (#2)
Targeted digital surveillance > Authentication bypass (#2)
Targeted digital surveillance > Malware (#2)

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[51]. The sabotage,

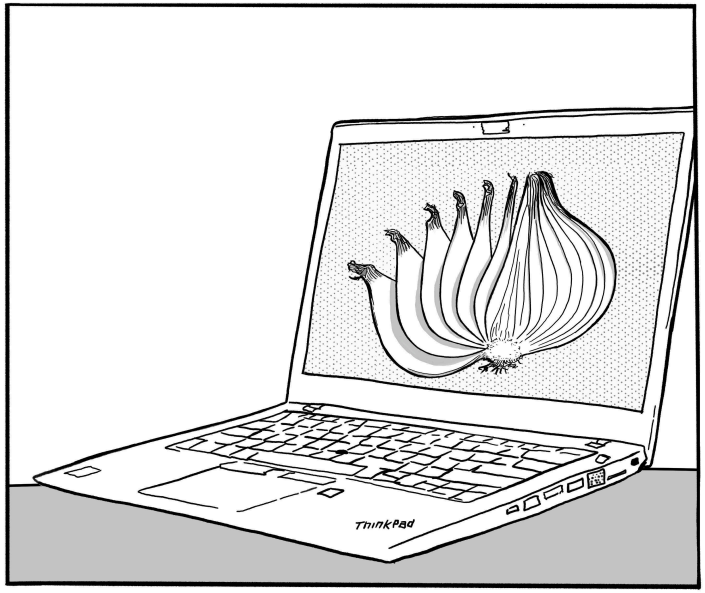
[50]https://notrace.how/resources/#wir-haben-eine-verabredung
[51]https://sansnom.noblogs.org/archives/16978

See Dna You Say? Burn Everything to Burn Longer: A Guide to Leaving No Traces[16] for protocol suggestions, and the DNA topic[17].

5.15. Digital best practices

Techniques addressed by this mitigation:

Alarm systems (#2)
Covert surveillance devices > Video (#2)
Door knocks (#2)
Forensics > Digital (#2)
Mass surveillance > Mass digital surveillance (#2)
Network mapping (#2)
Service provider collaboration (#2)
Targeted digital surveillance > Authentication bypass (#2)
Targeted digital surveillance > Malware (#2)
Targeted digital surveillance > Network forensics (#2)
Targeted digital surveillance > Physical access (#2)



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

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

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

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

- Use a GrapheneOS smartphone with end-to-end encrypted messaging applications. Do not use traditional SMS and calls.
- Leave it at home to mitigate location tracking.

Use security-oriented operating systems

Use:

- Debian[18] or Qubes OS[19] for daily computer use.
- Tails[12] 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. Tails is an operating system installed on a USB stick. It is unique in that it is designed for anonymity and leaves no trace on your computer[20]. All Internet connections are forced through the Tor network[21], and everything runs in the computer's memory (which is irrecoverable after the computer is shut down). See the official website[12] for easy-to-use installation instructions and great documentation.
- GrapheneOS[22] for phones.

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

[18] https://debian.org
[19] https://qubes-os.org
[20] https://tails.boum.org/about/index.en.html
[21] https://torproject.org
[22] https://grapheneos.org

tell with a high degree of confidence whether a tracking device is present or not.

[49] https://notrace.how/resources/#quelques-premiers-elements-du-dossier-d-enquete-contre-ivan

- 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 will 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.

5.32. Transportation by bike

Techniques addressed by this mitigation:

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

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

Advantages of transportation by bike include:

- Bikes are more difficult to identify through **video surveillance (#2)** than cars: the make and model of a bike can be obscured and bikes usually have no license plates.
- It is harder for a **mobile physical surveillance effort (#2)** to follow a bike than a car or someone on foot, especially without being detected, and it is easier to conduct **surveillance detection (p. 43)** and **anti-surveillance (p. 9)** from a bike. For example, in a six-month **physical surveillance (#2)** operation against a comrade in France, the police regularly lost track of him while he was biking[49].
- There are far fewer places to install a **tracking device (#2)** on a bike than on a car, and when you **search (p. 15)** a bike, you can

Encrypt your devices

Enable **Full Disk Encryption (p. 28)** on all your digital devices.

Use strong passwords

Most of your passwords (e.g. passwords you use to log in to websites) should be generated by and stored in a password manager—we recommend KeePassXC[23]—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[24] passwords of 5 to 7 words[25]. You can generate such passwords with KeePassXC (select the "Passphrase" tab when generating a password) or with physical dice[28]. You should use different passwords for each of your encrypted devices, but you can use the same password for all your KeePassXC databases.

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 7 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 7-word Diceware password. You don't memorize this 7-word

[23] https://keepassxc.org

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

[25] Use 5 words to be safe *right now*, and 7 words to be safer *in the future*. This recommendation is based on the assumption that you use the operating systems we recommend, on our best knowledge of our adversaries' capabilities, and on time[26] and cost[27] estimates of brute-forcing modern cryptosystems.

[26] https://blog.elcomsoft.com/2020/08/breaking-luks-encryption

[27] https://blog.1password.com/cracking-challenge-update

[28] https://www.eff.org/dice

password, you store it in the KeePassXC databases of one or two trusted comrades who also follow these digital best practices. This way, if you forget a password, you can ask the trusted comrades for the 7-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 14-word Diceware password. You don't memorize this 14-word password, you split it into two halves of 7 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 14-word password, and retrieve the USB stick: on it, you will find the forgotten password.

Use Tor or a VPN

Use Tor[21] 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 more difficult 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 more difficult for them to target you with **malware (#2)**).

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.

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 (#2)** by an adversary.

Tamper-evident preparation can be used:

- To detect if an adversary has accessed an electronic device during a **covert house search (#2)** (in which case they may have installed **malware (#2)** on the device).
- To detect if an adversary has accessed a **stash spot or safe house (p. 41)**.

Examples of tamper-evident preparation techniques include:

- Applying nail polish to a laptop screws and taking pictures of the screws. Because nail polish has a complex pattern, it will be very difficult for an adversary to remove the screws 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 opened.

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 effort. 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 effort.

See also

See the physical surveillance topic[4] and the related mitigation **Anti-surveillance (p. 9)**.

5.31. Tamper-evident preparation

Techniques addressed by this mitigation:

Targeted digital surveillance > Authentication bypass (#2)
Targeted digital surveillance > Physical access (#2)

- If you cannot use Tor for a given non-sensitive Internet activity (for example because you need to use a website that blocks Tor), you can use a VPN for it.
- You should not conduct any Internet activity without Tor or a VPN.

Unless you really know what you are doing, do not use both Tor and a VPN simultaneously[29].

Use end-to-end encrypted messaging applications

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

- Ideally, use decentralized and metadata-resistant applications such as Cwtch[31] or Briar[32].
- 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[33].

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. 28)**. 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.

[29] For more information on the benefits and drawbacks of doing this, see here[30].

[30] https://gitlab.torproject.org/legacy/trac/-/wikis/doc/TorPlusVPN

[31] https://cwtch.im

[32] https://briarproject.org

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

The advantage of the on-site backup is that it has a more recent version of your data. The advantage of the off-site backup is that it cannot be seized in the event of a **house raid (#2)** against your home.

Store your devices in a tamper-evident way

If an adversary physically accesses one of your digital devices, they could tamper with it, making it unsafe to use. To detect when an adversary has physically accessed a device, you can use **tamper-evident preparation (p. 45)**.

Buy your devices anonymously

Buying digital devices anonymously (p. 8) has two advantages:

- If one of your digital devices is seized by an adversary, the adversary may recover information from the device using **digital forensics (#2)**. If you bought the device anonymously, the adversary may not be able to link the device, and thus the information they recovered, to you.
- If you buy a digital device in a way that doesn't give you immediate access to the device (e.g. if you order a laptop online), buying anonymously can prevent an adversary that is targeting you from tampering with the device before you gain access to it (e.g. between the purchase and the delivery of the laptop).

If necessary, physically destroy your storage devices

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. 28)** using a strong password, an adversary could **bypass the encryption (#2)**.
- Modern storage devices can store a hidden copy of their data in *spare memory cells*[34], so overwriting the entire device is not sufficient.

this illogical route (such as stopping at a store along the route), so that a surveillance effort 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 is 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 effort 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 effort, 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 effort. 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 effort, 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 effort). To accomplish this, the third party can use

- Practice **tamper-evident preparation (p. 45)** to ensure that the stash spot or safe house hasn't been accessed by an adversary.

5.30. Surveillance detection

Techniques addressed by this mitigation:

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

Surveillance detection is the practice of detecting if you are under **physical surveillance (#2)**, 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 effort 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

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.

5.16. Encryption

Techniques addressed by this mitigation:

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

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

You can encrypt "in motion" data by using Tor[21] or a Virtual Private Network (VPN) for your Internet activity, and by using **end-to-end encrypted messaging applications (p. 22)** for your digital communications. Encrypting "in motion" data can prevent an adversary from monitoring your digital activity in various ways.

[34]https://tails.net/doc/encryption_and_privacy/secure_deletion/index.en.html

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. 36)**.

5.17. Fake ID

Techniques addressed by this mitigation:

ID checks (#2)
Network mapping (#2)

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 prevent **network mapping (#2)** or avoid arrest in the event of an **ID check (#2)**.
- To establish a **safe house (p. 41)**.
- To take the path of **clandestinity (p. 18)**.

5.18. Gloves

Techniques addressed by this mitigation:

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

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. 20)** 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. 29)** 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 hunting cameras were installed to monitor a forest stash spot[48]. Because of this, when accessing a stash spot or safe house, you can:

- Practice **anti-surveillance (p. 9)** to counter the risk of physical surveillance.
- **Dress anonymously (p. 5)** to counter the risk of being observed or recorded.

[48] 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

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 (#2)** coverage and a suitable place to change clothing before the action.
- Inspecting the action site itself, looking for surveillance cameras, **guards (#2)**, **alarm systems (#2)** and opportunities to attack the target.

When conducting physical reconnaissance, you can:

- Practice **anti-surveillance (p. 9)** to counter the risk of physical surveillance.
- **Dress anonymously (p. 5)** to counter the risk of being observed or recorded.

Digital reconnaissance

Examples of digital reconnaissance include:

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

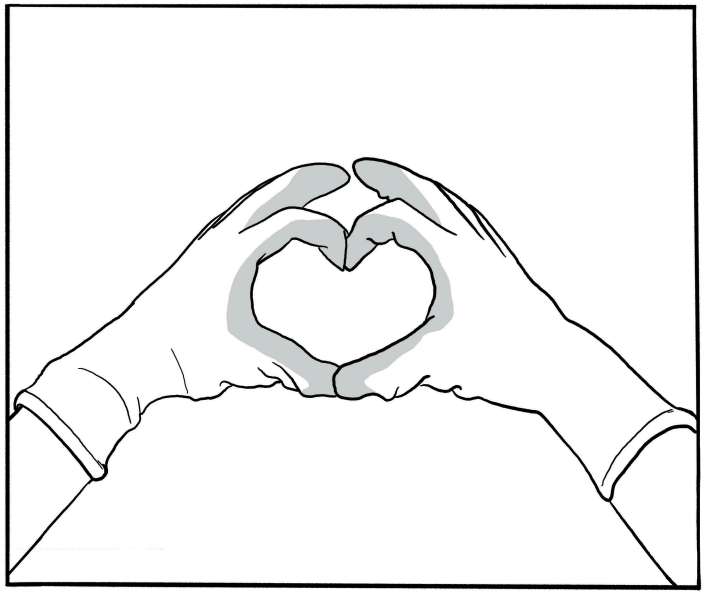
When conducting digital reconnaissance, you should follow **digital best practices (p. 22)**.

5.29. Stash spot or safe house

Techniques addressed by this mitigation:

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

Stash spots and safe houses are two ways to store incriminating materials. If incriminating materials are stored in a stash spot or safe house instead of in your home, they won't be found by an adversary in the event of a **house raid (#2)** or **covert house search (#2)**. A stash



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[35]).
- Do not use work gloves by themselves because they are generally permeable, and can let your sweat (and therefore your DNA) out.

And take appropriate precautions:

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

- 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[36].
- 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. 20)**.

Hand characteristics

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

Additional considerations

When using gloves, you should be aware that:

- You can leave fingerprints on the inside of gloves you wear, depending on their material.
- You leave DNA on the inside of gloves you wear.

[36] 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.

5.27. Prisoner support

Techniques addressed by this mitigation:
Informants (#2)

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

Common prisoner support initiatives include:

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

5.28. Reconnaissance

Techniques addressed by this mitigation:
Alarm systems (#2)
Guards (#2)
Mass surveillance > Video surveillance (#2)
Police patrols (#2)

Reconnaissance is the gathering of information about the target of an action. It precedes **action planning (p. 17)**. It can be done either physically (e.g., by traveling to the action site to inspect it) or digitally (e.g., by researching the target on the web). You should take into account the techniques an adversary may use against you during reconnaissance as much as you take them into account during the action itself.

Physical reconnaissance

5.26. Preparing for repression

Techniques addressed by this mitigation:

Extra-legal violence (#2)
House raid (#2)

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

Examples of practical preparation include:

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

Examples of psychological preparation include:

- 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[47] where he secluded himself in a house in the mountains for a month to prepare for the possibility of his imprisonment.

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

- 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[37].
- Handschuhe[38] (in German).

5.19. Masking your writing style

Techniques addressed by this mitigation:

Forensics > Linguistics (#2)

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

For example:

- You can write with brevity and intent.
- Before publishing a text, you can check it for spelling and grammatical errors to ensure that it does not contain any unique errors that could be traced back to you.
- To identify someone as the author of a text, an adversary can look for samples of that person's writing to use for comparison. To mitigate this, you can avoid keeping unencrypted samples of your writing at home that might be found in a **house raid (#2)** or **covert house search (#2)**, and generally avoid publishing texts in your name throughout your life.

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

See Counteracting Forensic Linguistics[39] and Who wrote that?[40].

5.20. Metadata erasure and resistance

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

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

Examples of metadata 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[41] that identifies the make and model of the printer that printed it.

For digital files, metadata erasure can be accomplished using MAT2[42] or similar software. Some **security-oriented operating systems (p. 22)** include metadata erasure tools by default.

Examples of metadata resistance include:

- Using a dedicated operating system (e.g. a Tails[12] 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.

[39] https://anonymousplanet.org/guide.html#appendix-a4-counteracting-forensic-linguistics
[40] https://notrace.how/resources/#wer-schreibt-denn-da
[41] https://eff.org/issues/printers
[42] https://github.com/tpet/mat2

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

5.25. Preparing for house raids

Techniques addressed by this mitigation:
Covert house search (#2)
House raid (#2)

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

An important precautionary measure is to minimize the presence of materials 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. 28)**, 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. 41)**, 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 specific guides to sketchy things.

In addition, to detect if an adversary has **physically accessed (#2)** an electronic device during a covert house search, you can use **tamper-evident preparation (p. 45)**.

(#2) operation (with effective ranges of up to 300 meters). For example, in Italy in 2019[46] 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. 33)** 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[44].

5.24. Physical intrusion detection

Techniques addressed by this mitigation:

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

Physical intrusion detection is the process of detecting when an adversary enters or attempts to enter a space, for example for a **covert house search (#2)**. You can do this by making sure there is always someone in the space who would notice if an adversary tried to enter, or by monitoring the space with a video surveillance system.

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

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

- Using metadata-resistant messaging applications such as Cwtch[31] or Briar[32].

5.21. Need-to-know principle

Techniques addressed by this mitigation:

Evidence fabrication (#2)
Infiltrators (#2)
Informants (#2)
Network mapping (#2)

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 the action or speculating about the involvement of others, tell them to stop.

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

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

See also:

- Secrets And Lies[43] about the effects that secrecy can have on an individual and collective level.
- The security culture topic[44].

5.22. Network map exercise

Techniques addressed by this mitigation:

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

A network map exercise consists of creating a graphical representation of the links between you and the people in your network in order to critically examine those links. This exercise is designed to sharpen your ability to make informed and critical choices about the people you associate with, with the ultimate goal of making your network more resilient to **infiltration (#2)** attempts.

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

For instructions on how to do this, see Stop hunting sheep: a guide to creating safer networks[45]. Such a network map would be invaluable

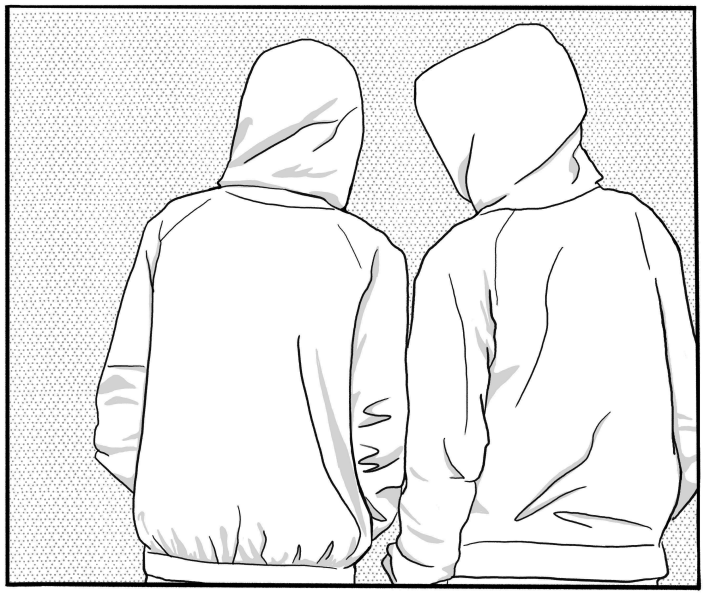
[43] https://notrace.how/resources/#secrets-and-lies
[44] https://notrace.how/resources/#topic=security-culture
[45] https://notrace.how/resources/#stop-hunting-sheep

to an adversary; it is essentially what they construct during **network mapping (#2)**, so it should be burned immediately after use.

5.23. Outdoor and device-free conversations

Techniques addressed by this mitigation:

Covert surveillance devices > Audio (#2)
Mass surveillance > Video surveillance (#2)



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

Outdoor and device-free conversations are necessary because:

- Indoor spaces, including cars can contain **covert surveillance devices (#2)**.
- Electronic devices can be infected with **malware (#2)** that can turn them into covert microphones.

Outdoor conversations can be recorded with covert microphones or long-range parabolic microphones during a **physical surveillance**